Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Cybersecuritybeeld Nederland

CSBN 2015



Cybersecuritybeeld Nederland

CSBN 2015

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast biedt het NCSC informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

Het NCSC is een onderdeel van de Directie Cyber Security van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Samenwerking en bronnen

Bij het opstellen van dit rapport heeft het NCSC dankbaar gebruik gemaakt van informatie die de volgende partijen beschikbaar hebben gesteld:
- De ministeries
- MIVD
- DefCERT
- AIVD
- Team High Tech Crime, politie
- Openbaar Ministerie
- Vertegenwoordigers van de vitale sectoren
- NCTV
- Nationale Beheersorganisatie Internet Providers
- Platform Internetstandaarden
- Bits of Freedom
- Nederland ICT
- Betaalvereniging Nederland
- VNO-NCW
- Wetenschappelijke instellingen
- Universiteiten
- Experts uit het cybersecuritywerkveld

Hun bijdragen, inhoudelijke reviews, openbaar toegankelijke bronnen, informatie van de vitale sectoren en analyses van het NCSC hebben samen bijgedragen aan de inhoudelijke kwaliteit van het beeld.

Inhoud

Samenvatting

Jaarlijks publiceert het Nationaal Cyber Security Centrum het Cybersecuritybeeld Nederland (CSBN). Het CSBN komt in nauwe samenwerking met publieke en private partners tot stand. Doel is het bieden van inzicht in ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van cybersecurity over de periode april 2014 tot en met april 2015.

De focus van het CSBN ligt op de ontwikkelingen in Nederland. Ook belangwekkende ontwikkelingen in het buitenland zijn meegenomen. Het CSBN is een feitelijke beschrijving, met duiding op basis van inzicht en expertise vanuit overheidsdiensten, vitale sectoren en wetenschap. Voor dit CSBN werkte het NCSC opnieuw samen met een groot aantal partijen, zowel publiek (bijvoorbeeld politie, inlichtingen- en veiligheidsdiensten en het Openbaar Ministerie), wetenschappelijk, als privaat (zoals de vitale sectoren).

In de afgelopen jaren groeide de aandacht voor de afhankelijkheid van ICT. Landen hechten steeds meer belang aan het internet en ICT wordt vaker onmisbaar. Het inzicht in het aantal incidenten begint toe te nemen, waarmee ook het nemen van maatregelen om cybersecurity te vergroten gerichter kan gebeuren, voor grotere en kleinere organisaties. Phishing en cryptoware blijven echter een bedreiging voor heel Nederland.

Kernbevindingen

Cryptoware en andere ransomware is het cybercriminele businessmodel bij uitstek

Criminelen zetten cryptoware (gijzelvirussen) steeds vaker in om hun doeleinden te bereiken. In tegenstelling tot andere veelvoorkomende malware, zoals Remote Access Tools (RAT's), blokkeren de criminelen met cryptoware de toegang tot gegevens met behulp van encryptie. De bereidheid van mensen en organisaties om de criminelen te betalen, zorgt voor hoge gemiddelde opbrengsten per doelwit voor criminelen. Zij kunnen daarom relatief veel investeren per infectie. Ook geavanceerdere vormen, bijvoorbeeld gericht op webapplicaties, zijn inmiddels waargenomen. De komende jaren neemt de populariteit van het gebruik van ransomware en (vooral) cryptoware verder toe.

Geopolitieke spanningen manifesteren zich steeds vaker in (dreigende) inbreuken op digitale veiligheid

Staten en andere actoren die in lijn met het belang van deze staten lijken te acteren, maken steeds vaker gebruik van digitale aanvallen en cyberoperaties. Het doel is om hun belangen te behartigen en om geopolitieke verhoudingen of ontwikkelingen te beïnvloeden. Digitale aanvallen zijn een aantrekkelijk alternatief voor en aanvulling op conventionele militaire en spionagemiddelen.
Ze hebben een grote omvang en impact tegen lage kosten en afbreukrisico's. Conflicten, aanslagen of politieke gevoeligheden waren het afgelopen jaar veelvuldig aanleiding voor digitale aanvallen. Daarbij is vaak lastig te herleiden wie de actor is die de daadwerkelijke aanval uitvoert, en in hoeverre een statelijke actor hierbij een aansturende rol speelt.

Phishing wordt veel gebruikt in gerichte aanvallen en is dan voor gebruikers nauwelijks te herkennen

Phishing (het 'vissen' naar inlog- en andere gegevens van gebruikers) speelt een sleutelrol bij het uitvoeren van gerichte digitale aanvallen. Phishing-e-mails in gerichte aanvallen zijn voor gebruikers vaak nauwelijks te herkennen. Met een geslaagde phishingcampagne krijgen aanvallers toegang tot interne netwerken van organisaties en de daar opgeslagen informatie. Middelen om authentieke e-mail als zodanig herkenbaar te maken (zoals digitale handtekeningen, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) en Domain-based Message Authentication, Reporting, and Conformance (DMARC)) worden in de praktijk slechts beperkt toegepast. Dit zorgt ervoor dat phishing een laagdrempelige en effectieve aanvalsmethode blijft voor aanvallers.

Beschikbaarheid wordt belangrijker nu alternatieven voor ICT-systemen verdwijnen

Belangrijke maatschappelijke processen vallen stil als de bijbehorende ICT-systemen en analoge alternatieven niet beschikbaar zijn. Het verdwijnen van analoge alternatieven voor ICT-systemen maakt de beschikbaarheid van deze systemen daarom nog belangrijker. Dit is vooral het geval waar deze ICT-systemen belangrijke maatschappelijke processen zoals transport, financieel verkeer of energievoorziening ondersteunen. De maatregelen die banken hebben getroffen tegen DDoS-aanvallen tonen aan dat het mogelijk is effectieve maatregelen te treffen om beschikbaarheid van digitale voorzieningen te verhogen. Organisaties treffen dergelijke maatregelen echter vaak pas als de ICT-systemen al beschikbaarheidsproblemen hebben gekend.

Kwetsbaarheden in software zijn nog altijd de achilleshiel van digitale veiligheid

Software is een cruciaal onderdeel van onze digitale infrastructuur, omdat software de mogelijkheden van hardware en de steeds groeiende hoeveelheid data ontsluit. Ook dit jaar brachten softwareleveranciers duizenden updates uit om kwetsbaarheden in hun software te repareren. De belemmeringen die organisaties ervaren bij het installeren van updates, zorgen ervoor dat ze het installeren ervan soms achterwege laten. Zolang de updates niet geïnstalleerd zijn, blijven delen van hun netwerk kwetsbaar. Actoren die bijvoorbeeld via phishing of zero-daykwetsbaarheden binnendringen, bewegen zich door zulke kwetsbaarheden verder door het netwerk. Met software op nieuwe plaatsen, zoals medische apparatuur of als onderdeel van het Internet der Dingen, neemt het belang van veiligheid verder toe. Helaas blijkt de software in deze apparaten regelmatig elementaire kwetsbaarheden te bevatten. Updates, die vaak handmatig geïnstalleerd moeten worden, zijn door de aard van deze apparaten niet eenvoudig te installeren.

Hoofdvragen

De hoofdvragen van dit CSBN 2015 zijn:
- Welke gebeurtenissen of welke activiteiten van welke actoren kunnen ICT-belangen aantasten, welke hulpmiddelen gebruiken zij en welke ontwikkelingen doen zich daarbij voor? (**dreigingen**)
- In hoeverre is Nederland weerbaar tegen kwetsbaarheden in ICT, kunnen die leiden tot aantasting van ICT-belangen en welke ontwikkelingen doen zich daarbij voor? (**weerbaarheid**)
- Welke Nederlandse belangen worden in welke mate geschaad door beperkingen van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie en welke ontwikkelingen doen zich daarbij voor? (**belangen**)

Inzicht in dreigingen en actoren

Tabel 1 geeft inzicht in de dreigingen die de verschillende actoren over de periode april 2014 tot en met april 2015 vormden voor de doelwitten 'overheden', 'private organisaties' en 'burgers'. Criminele organisaties en statelijke actoren blijven een dreiging vormen voor deze drie doelwitcategorieën. Deze dreiging is specifieker geworden. De manifestaties van minder geavanceerde actoren vormen voor de meeste organisaties een kleiner deel van het totaal dan voorheen. De rode kleur verhult in sommige gevallen dat ook een hoog dreigingsniveau kan groeien. De paragrafen over criminelen en statelijke actoren in Hoofdstuk 2 gaan hier verder op in.

Manifestaties

Groei van aantal incidenten met ransomware en cryptoware zet door

De opkomst van ransom- en cryptoware in 2013 heeft zich in 2014 en 2015 voortgezet, ook in Nederland. Ransom- en cryptoware is malware die ICT-systemen 'gijzelt' door ze niet beschikbaar te maken en om losgeld vraagt. Cryptoware versleutelt daarnaast de opgeslagen gegevens. Diverse cryptowarevarianten zorgden de afgelopen periode voor veel incidenten. Besmettingen vonden plaats door bijvoorbeeld Cryptolocker, CryptoFortress, Cryptowall en CTB-locker. In Nederland worden organisaties vaak getroffen door dergelijke besmettingen.

DDoS-aanvallen blijven plaatsvinden, maar maatregelen voorkomen vaker verstoringen

In Nederland blijven DDoS-aanvallen een punt van aandacht. Na de golf van DDoS-aanvallen begin 2013 investeerden dienstaanbieders in maatregelen om deze af te wenden. Er worden nog steeds frequente en zware DDoS-aanvallen op sites van overheden en private organisaties gedetecteerd. De oorzaak van de problematiek blijft dus bestaan. De toegenomen aandacht voor anti-DDoS-maatregelen zorgt er echter voor dat de dienstverlening in veel gevallen niet verstoord raakt.

Spionageaanvallen, die steeds frequenter worden, beginnen met spearphishing

Het afgelopen jaar kreeg Nederland veel vaker te maken met digitale spionageaanvallen die een dreiging voor de nationale veiligheid en economische belangen vormen. Uit onderzoek van de AIVD en de MIVD bleek dat Nederlandse overheidsinstellingen in 2014 veelvuldig doelwit waren van geavanceerde digitale spionageaanvallen. Het merendeel van deze aanvallen is uitgevoerd met spearphishing-e-mails die met malware besmette bijlagen of links naar websites met malware bevatten.

Tabel 1 **Dreigingsmatrix**

	Doelwitten		
Bron van Dreiging	**Overheden**	**Private organisaties**	**Burgers**
Beroepscriminelen	Diefstal en publicatie of verkoop van informatie ↘	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie
	Manipulatie van informatie	Manipulatie van informatie	Manipulatie van informatie
	Verstoring van ICT	Verstoring van ICT	Verstoring van ICT
	Overname van ICT	Overname van ICT ↘	Overname van ICT
Staten	Digitale spionage	Economische spionage	Digitale spionage
	Offensieve cybercapaciteiten	Offensieve cybercapaciteiten ↗	
Terroristen	Verstoring/overname van ICT	Verstoring/overname van ICT	
Cybervandalen en scriptkiddies	Diefstal van informatie	Diefstal van informatie	Diefstal van informatie ↗
	Verstoring van ICT	Verstoring van ICT	
Hacktivisten	Diefstal en publicatie van verkregen informatie	Diefstal en publicatie van verkregen informatie	↘
	Defacement	Defacement	
	Verstoring van ICT	Verstoring van ICT	
	Overname van ICT	Overname van ICT ↘	
Interne actoren	Diefstal en publicatie of verkoop van verkregen informatie	Diefstal en publicatie of verkoop van verkregen informatie	
	Verstoring van ICT	Verstoring van ICT	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private Organisaties		Diefstal van informatie (bedrijfs-spionage)	Commercieel gebruik, misbruik of ‘doorverkopen’ van gegevens
Geen actor	Uitval van ICT	Uitval van ICT	Uitval van ICT

↘ ↗	Laag	Midden	Hoog
Verandering ten opzichte van CSBN-4	*Er zijn geen nieuwe trends of fenomenen waar de dreiging van uitgaat.* OF *Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen.* OF *Er deden zich geen noemenswaardige incidenten van de dreiging voor in de rapportageperiode.*	*Er zijn nieuwe trends en fenomenen waargenomen waar de dreiging van uitgaat.* OF *Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen.* OF *Incidenten deden zich voor buiten Nederland, enkele kleine in Nederland.*	*Er zijn duidelijke ontwikkelingen die de dreiging opportuun maken.* OF *Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft.* OF *Incidenten deden zich voor in Nederland.*

Dreigingen: Actoren

De grootste dreiging blijft uitgaan van beroepscriminelen en statelijke actoren

Criminelen ontwikkelen hun digitale vaardigheden steeds verder. Het afgelopen jaar stond bijvoorbeeld in het teken van enkele digitale aanvallen door criminelen die opvielen door hun goede organisatie, nauwkeurige uitvoering en technische geavanceerdheid. Daarnaast voeren er meer landen digitale aanvallen op of via de infrastructuur van Nederlandse organisaties uit. De grootste digitale spionagedreiging komt van buitenlandse inlichtingendiensten.

Terroristen vormen nog geen grote dreiging, maar hun capaciteiten groeien wel

Hoewel de potentie op digitaal gebied van terroristische actoren groeit, vormen ze nog geen grote dreiging vanwege hun beperkte technische capaciteiten. Er zijn geen aanwijzingen voor een concrete dreiging richting Nederland. In het kader van digitale aanvallen door terroristen gaat de grootste dreiging op dit moment uit van het jihadisme. Tot nu toe bleven digitale aanvallen met jihadistische motieven in Nederland beperkt tot kleinschalige aanvallen waar weinig kennis en menskracht voor nodig was.

Conflicten, aanslagen en incidenten vormen context voor digitale aanvallen

Verschillende actoren grijpen intra- en internationale conflicten, aanslagen en incidenten vaak aan als aanleiding voor digitale aanvallen. Het afgelopen jaar zijn er bijvoorbeeld veel digitale aanvallen en cyberoperaties waargenomen die in geopolitieke context geplaatst kunnen worden, zoals de malware-aanvallen gerelateerd aan het conflict in Oekraïne. Deze aanvallen zijn vaak erg moeilijk aan partijen toe te schrijven. Zowel statelijke actoren als activistische hackers met patriottische motieven hebben de intenties en de middelen om deze aanvallen uit te voeren.

Dreigingen: Middelen

Verspreiding van cryptoware is een lucratieve criminele activiteit

De opbrengsten die criminelen realiseren met cryptoware zijn hoog. Circa 10 procent van de Nederlandse aangevers zegt betaald te hebben om toegang tot bestanden terug te krijgen. Vermoedelijk is de opbrengst van een betaling enkele honderden euro's per persoon. De betrokken criminelen doen hun best om hun markt te vergroten door te zoeken naar andere middelen om te besmetten (zoals SD-kaarten, USB-sticks en netwerkbronnen) en door andere methoden van versleutelen (bijvoorbeeld door over lange periode systemen te corrumperen).

Phishing, in het bijzonder spearphishing, is hét middel voor gerichte aanvallen

De daders van diverse gerichte aanvallen die afgelopen tijd bekend werden slaagden vaak in hun opzet door gebruik te maken van spearphishing, waarbij één persoon of een beperkte groep personen een phishing-e-mail ontvangt. Naast spearphishing gebruiken actoren ook nog altijd klassieke phishing als hulpmiddel. Opvallend is dat Nederland een populair doelwit is voor phishers. Dat kan te maken hebben met de relatief goede economische situatie en de sterke euro.

Malafide advertenties blijven een gevaar voor internetgebruikers

Advertenties zijn verwerkt in veel websites, die soms hoge bezoekersaantallen hebben. Eén malafide advertentie kan daarom in korte tijd een groot effect sorteren. Het openen van een website met daarop een malafide advertentie leidt er in veel gevallen toe dat geheel automatisch – dus zonder verdere handeling van de gebruiker – allerlei kwetsbaarheden op het systeem van de gebruiker worden uitgebuit. Cybercriminelen misbruiken advertentienetwerken tegenwoordig ook om een specifieke groep van gebruikers aan te vallen. Hiervoor maken zij gebruik van online advertentieveilingen.

Weerbaarheid: Kwetsbaarheden

Grote publiciteit voor sommige kwetsbaarheden maakt prioriteren lastig

In de afgelopen rapportageperiode is een ontwikkeling te zien waarbij er veel meer publiciteit is rondom technische kwetsbaarheden. Uit verschillende sectoren komen signalen dat er een risico schuilt in deze publiciteitscampagnes: door de grote aandacht voor individuele kwetsbaarheden kan de waan van de dag de aandacht afleiden van structurele oplossingen. Bestuurders nemen dan niet altijd beslissingen op basis van de juiste informatie. In de organisaties ontstaat dan het beeld dat de informatiebeveiligers onvoldoende voorbereid zijn.

Het lukt niet om phishing met alleen bewustwording te bestrijden

De kwaliteit van de phishingteksten is steeds beter geworden. Het is gebruikers bijna niet meer kwalijk te nemen dat ze hierin trappen. Technische maatregelen om phishing tegen te gaan worden echter nog maar beperkt gebruikt. Minder dan tien procent van de domeinnamen van de overheid is bijvoorbeeld beschermd tegen phishingaanvallen met behulp van de open standaarden DKIM, SPF en DMARC.

Weerbaarheid: Maatregelen

Ook beveiliging van opensourcesoftware kost geld

De Heartbleed-kwetsbaarheid maakte duidelijk dat opensourcesoftware niet automatisch veiliger is, zelfs als die veel gebruikt wordt. De publiciteit rond deze bug leidde er in april 2014 toe dat grote internetbedrijven de handen ineensloegen in het Core Infrastructure Initiative. Binnen deze structuur wordt geïnvesteerd in de opensource-basisinfrastructuur van

het internet. Dit initiatief verbetert de basisbeveiliging van het internet. Het bestrijkt echter momenteel slechts een klein deel van de opensourceprojecten die de infrastructuur van het internet dragen. Voor andere projecten is financiering niet in deze mate beschikbaar.

Werven in cybersecurity: veel vacatures, weinig mensen

De arbeidsmarkt voor cybersecurityprofessionals kenmerkt zich al langer door een groot verschil tussen de vraag naar en het aanbod van (technische) cybersecurityprofessionals. Het aantal vacatures neemt toe; ook de overheid heeft in de afgelopen periode medewerkers op dit terrein geworven. Organisaties hebben regelmatig moeite om vacatures te vervullen. Dat geldt in het bijzonder voor technische cybersecurityfuncties.

Detectiecapaciteit is essentieel om geavanceerde aanvallen te ontdekken

Geavanceerde aanvallen, zogeheten Advanced Persistent Threats (APT's), zijn lastig te detecteren. Deze aanvallen, die gericht zijn op organisaties in verschillende sectoren, omzeilen structureel bestaande beveiligingsmaatregelen. De aanvallen blijven vaak maanden tot jaren onopgemerkt, wat kan leiden tot een enorme omvang en impact van de schade voor de getroffen organisaties. Hoewel steeds meer organisaties speciale software hebben draaien die hen tegen APT's moeten beschermen, lijkt het weren ervan voor veel organisaties een grotendeels onontgonnen gebied.

Belangen

Nieuwe toepassingsgebieden leveren kwetsbaarheden en debat op

Auto's, vliegtuigen en andere vervoermiddelen worden voorzien van meer ICT-mogelijkheden. Dat vraagt om aandacht voor de beveiliging ervan. Het is immers niet de bedoeling dat een beveiligingsprobleem in een entertainmentsysteem gevolgen heeft voor de besturing van het voertuig. Een gebrek aan beveiliging zou in een dergelijk geval zelfs fatale gevolgen kunnen hebben. Dergelijke risico's kunnen ook ontstaan als de gebruikte software bugs bevat, een licentie verloopt of een netwerkdienst niet meer bereikbaar is. Beveiliging heeft vaak geen prioriteit bij het ontwikkelen van dergelijke nieuwe toepassingen.

Belangen van vitale sectoren zijn groot maar stabiel

De belangen die de vitale sectoren beschermen blijven groot en veranderen weinig. Dat blijkt uit gesprekken met vertegenwoordigers van organisaties in deze sectoren. Hoewel het beveiligen van informatie en systemen telkens nieuwe uitdagingen creëert, zijn de achterliggende motivaties voor het beveiligen nauwelijks veranderd.

Alternatieven voor ICT-systemen verdwijnen

Wanneer ICT-systemen voor de ondersteuning van maatschappelijke processen niet beschikbaar zijn, is er in een groeiend aantal gevallen geen analoog alternatief meer. De beschikbaarheid van deze ICT-systemen wordt daarmee belangrijker: uitval is geen optie. Tegelijkertijd is de onderliggende technologie complexer dan bij analoge systemen. Ook zijn deze systemen gemakkelijker aan te vallen als ze via het internet bereikbaar zijn.

Inleiding

Het onderwerp cybersecurity krijgt een steeds prominentere plaats in Nederland. Dit jaar was Nederland gastheer van de internationale Global Conference on Cyber Space. Zo kon Nederland zich presenteren als voorloper op het gebied van cybersecurity. Tegelijkertijd onderstreepten vele incidenten met gekraakte databases en kwetsbaarheden in de infrastructuur van overheden en bedrijven het dagelijkse belang van cybersecurity. Wereldwijd waren beeldbepalende incidenten aanleiding tot verhoogde media-aandacht, zoals de Sony-hack en een hack op de Amerikaanse bank JPMorgan Chase. Er lijkt in de publieke opinie sprake te zijn van een toenemende perceptie van cybercriminaliteit en hacken als dreigingen. Het is echter maar de vraag in hoeverre er sprake is van groei van de daadwerkelijke problemen.

De toenemende afhankelijkheid van internettoepassingen vertaalt zich er anno 2015 naar dat toegang tot internetgerelateerde diensten inmiddels vanzelfsprekend is, en daarmee onmisbaar. Het is inmiddels ondenkbaar dat ICT geen rol speelt bij allerlei alledaagse activiteiten, zoals financiële transacties, reizen en communicatie.

De centrale rol van internet en ICT werkt intussen ook door op het geopolitieke niveau. De toegenomen afhankelijkheid van ICT vertaalt zich in een toenemende druk om politiek greep te krijgen op datzelfde internet.

Jaarlijks publiceert het Nationaal Cyber Security Centrum het Cybersecuritybeeld Nederland (CSBN). Het CSBN komt tot stand in nauwe samenwerking met een groot aantal partijen, zowel publiek (bijvoorbeeld politie, inlichtingen- en veiligheidsdiensten en het Openbaar Ministerie), wetenschappelijk, als privaat (vitale sectoren).

Het CSBN biedt inzicht in de ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van cybersecurity in de afgelopen periode. Het is bedoeld voor beleidsmakers bij de overheid en bij de vitale sectoren, met als doel de digitale weerbaarheid van Nederland te versterken of lopende cybersecurityprogramma's te verbeteren.

De hoofdvragen in het CSBN 2015 zijn:
- Welke gebeurtenissen of welke activiteiten van welke actoren kunnen ICT-belangen aantasten, welke hulpmiddelen gebruiken zij en welke ontwikkelingen doen zich daarbij voor? (**dreigingen**)
- In hoeverre is Nederland weerbaar tegen kwetsbaarheden in ICT, kunnen die leiden tot aantasting van ICT-belangen en welke ontwikkelingen doen zich daarbij voor? (**weerbaarheid**)
- Welke Nederlandse belangen worden in welke mate geschaad door beperkingen van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie en welke ontwikkelingen doen zich daarbij voor? (**belangen**)

Het eerste hoofdstuk, Manifestaties, biedt een overzicht van inbreuken op cybersecurity van het afgelopen jaar. De volgende hoofdstukken analyseren deze ontwikkelingen en geven antwoorden op de hoofdvragen.

Dit CSBN bouwt voort op eerdere beelden en verwijst daar ook naar. Toch is het rapport een zelfstandig document. De rapportageperiode van het CSBN 2015 loopt van april 2014 tot en met april 2015. De focus ligt op de ontwikkelingen in Nederland. Ook belangwekkende ontwikkelingen in het buitenland zijn meegenomen.

Het CSBN is een feitelijke beschrijving met duiding op basis van inzicht en expertise van overheidsdiensten en de vitale sectoren zelf. Het beschrijft ontwikkelingen in kwalitatieve vorm en geeft, daar waar in betrouwbare vorm beschikbaar, een kwantitatieve onderbouwing en/of een verwijzing naar bronnen. Het monitoren van de ontwikkelingen is een continu proces met het CSBN als een van de jaarlijkse resultaten. Zaken die ten opzichte van de vorige edities niet of nauwelijks zijn veranderd, zijn niet of beknopt beschreven.

21 procent van 's werelds meest bezochte sites draait op software met bekende kwetsbaarheden.



1 Manifestaties

Het beeld van 2014 werd in hoge mate bepaald door een aantal omvangrijke incidenten waarbij grote hoeveelheden data op straat kwamen te liggen. Voorbeelden zijn de hacks bij Sony in november 2014 en TV5MONDE in maart 2015. Daarnaast waren geopolitieke ontwikkelingen (zoals het conflict in Oekraïne of de opkomst van ISIS) de oorzaak van veel manifestaties. Ook afpersing door criminele organisaties kwam veel voor. Dit werd het duidelijkst door de groeiende hoeveelheid besmettingen met verschillende vormen van cryptoware.

Dit hoofdstuk geeft een overzicht van de voornaamste manifestaties op cybersecuritygebied in de afgelopen rapportageperiode. Er is sprake van een manifestatie wanneer belangen worden geschaad, omdat een dreiging manifest wordt. De weerbaarheid is dan onvoldoende om de dreiging te kunnen tegengaan. Een kwaadwillende actor kan zo actief gebruik maken van een kwetsbaarheid in een systeem, maar manifestaties kunnen ook plaatsvinden door fouten van gebruikers en beheerders of door technische verstoringen.

Verstoring van ICT

Bedrijven en publieke organisaties zijn voor hun primaire proces steeds afhankelijker van ICT-middelen. Dit geldt ook voor burgers en hun dagelijks leven. Hierdoor nemen de nadelige consequenties bij de uitval ervan ieder jaar toe. Voor aanvallers is het moedwillig verstoren van ICT dan ook een belangrijk middel om tegenstanders of concurrenten schade te berokkenen of om bedrijven en individuele burgers af te persen.

Ransom- en cryptoware

De opkomst van ransom- en cryptoware in 2013 heeft zich in 2014 en 2015 voortgezet, ook in Nederland. Ransom- en cryptoware is malware die ICT-systemen 'gijzelt' door ze niet beschikbaar te maken en om losgeld vraagt. Cryptoware versleutelt daarnaast de opgeslagen gegevens. Diverse cryptoware-varianten hebben de afgelopen periode voor veel incidenten gezorgd. Besmettingen vonden plaats door bijvoorbeeld Cryptolocker, CryptoFortress, Cryptowall en CTB-locker. In Nederland worden kantoorautomatiseringsomgevingen vaak getroffen door dergelijke besmettingen. Dit beeld komt onder meer naar voren in gesprekken met vertegenwoordigers van de vitale sectoren. Besmettingen bij bijvoorbeeld de gemeenten Dronten[1], Lochem[2] en Den Haag[3] kwamen in het nieuws. Ook Rijkswaterstaat[4] was slachtoffer van cryptoware. De meeste besmettingen blijven buiten het nieuws, maar bij veel organisaties hebben ze in de afgelopen periode plaatsgevonden. Besmettingen vinden veelal plaats doordat medewerkers op het werk privé-e-mail lezen.[5] Berichten die zij daar ontvangen, bevatten de malware of verwijzen ernaar met een link. Cryptoware trof zowel publieke als private organisaties, waaronder zorginstellingen[6] en het mkb.[7] Sommige bedrijven betalen het gevraagde

1 https://www.security.nl/posting/422471/Ransomware+verstoorde+dienstverlening+Dronten
2 http://www.lochem.nl/bestuur-organisatie-nieuws/nieuws/nieuwsoverzicht/artikel/gemeente-lochem-getroffen-door-computervirus/
3 https://www.security.nl/posting/406204/Computers+gemeente+Den+Haag+besmet+via+valse+PostNL-mail
4 http://tweakers.net/nieuws/102028/computers-rijkswaterstaat-zijn-besmet-met-ransomware.html
5 Informatie verschillende ISAC's.
6 Informatie zorg-ISAC (20 maart 2015).
7 http://www.computable.nl/artikel/nieuws/security/5242994/1276896/cryptowarevirus-raakt-vooral-het-mkb.html

losgeld om de getroffen bestanden te kunnen herstellen.[8] De businesscase voor criminelen blijft hierdoor bestaan.

Het totaal aantal cryptowarebesmettingen is lastig te bepalen. Volgens het Amerikaanse beveiligingsbedrijf Dell SecureWorks heeft alleen al de variant Cryptowall medio 2014 in vijf maanden tijd wereldwijd ongeveer 625.000 computersystemen geïnfecteerd.[9] In Nederland zou het gaan om 1000 tot 5000 systemen. 'Ouderwetse' Kovter ransomware, waarbij gebruikers de boodschap krijgen dat illegaal materiaal is gedownload en dit kan worden afgekocht door het betalen van een boete, besmette op zijn hoogtepunt medio 2014 ruim 40.000 computers per dag.[10]

controlesystemen (ICS) manipuleert kan leiden tot schade aan gekoppelde productie- of controlesystemen. De inzet van Wiper-malware is beperkt en vooralsnog niet in Nederland waargenomen. Sabotageaanvallen op ICS zijn in Nederland tot op heden hoogst uitzonderlijk.[12]

In het jaarrapport 2014 van de Duitse BSI wordt melding gemaakt van sabotage bij een hoogovenbedrijf in Duitsland. De aanvallers zijn door middel van spearphishing in het kantoornetwerk van het bedrijf binnengedrongen. Vanuit dit netwerk konden zij zich toegang verschaffen naar het operationele control-netwerk van de hoogoven. Door het beschadigen van een oven legden zij

Casus Coinvault

De Nederlandse politie onderzoekt diverse cryptoware-aanvallen.[11] Van één van deze aanvallen, die gebruik maakt van de Coinvault-malware, heeft de politie in samenwerking met Kaspersky Lab een aantal servers van de criminelen ontdekt en nader onderzocht. Uit dit onderzoek blijkt dat de drie onderzochte servers gezamenlijk verantwoordelijk zijn voor 2081 besmettingen met Coinvault (zie onder).

Server	Aantal besmettingen	Besmettingen NL	Betaling losgeld
#1	718	48%	1,3%
#2	826	45%	2,1%
#3	537	56%	1,1%

Opvallend aan de malware is dat in bijna de helft van de gevallen sprake is van een Nederlands slachtoffer. Deze malware-variant heeft veel Nederlandse links. Naast de vele Nederlandse slachtoffers waarop de ransomware zich richt, gebruikt Coinvault Nederlandse plug-ins, is er een helpdeskpagina in foutloos Nederlands en verwijzen de criminelen voor betaling naar een Nederlandse bitcoinexchange.

Het blijkt dat ongeveer 1,5 procent van de slachtoffers daadwerkelijk heeft betaald om bestanden terug te krijgen. Een kanttekening daarbij is dat het genoemde percentage is gemeten op het moment dat de servers in beslag werden genomen. Vermoedelijk waren de aanvalscampagnes op dat moment één tot twee weken actief.

Sabotage

Door digitale sabotageaanvallen kunnen websites enige tijd onbereikbaar of onbruikbaar zijn. De meest voorkomende vormen van dergelijke sabotage zijn DDoS-aanvallen en defacements. Deze komen verderop in dit hoofdstuk aan bod. De maatschappelijke onrust en kosten voor de betrokkenen kunnen omvangrijk zijn. Dergelijke aanvallen resulteren echter veelal niet in permanente schade aan de aangevallen informatiesystemen.

Er vinden echter ook ernstiger vormen van sabotage plaats. Met Wiper-malware worden gegevens gewist en dat kan leiden tot verlies van informatie. Malware die industriële

vervolgens de productie enige tijd stil. Het is niet bekend wie er achter deze aanval zit.

(Distributed) Denial-of-Service-incidenten

In Nederland blijven DDoS-aanvallen een punt van aandacht. Na de golf van DDoS-aanvallen begin 2013 is er door dienstaanbieders geïnvesteerd in maatregelen om deze af te wenden. Er worden nog steeds frequente en zware DDoS-aanvallen op sites van overheden en private organisaties gedetecteerd. De oorzaak van de problematiek blijft dus bestaan. De toegenomen aandacht voor anti-DDoS-maatregelen zorgt er echter voor dat de dienstverlening in veel gevallen niet verstoord raakt. Begin 2015 was de

8 https://www.security.nl/posting/422024/Tientallen+Nederlandse+bedrijven+betalen+ransomware
9 http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/
10 http://landing.damballa.com/rs/damballa/images/Damballa_Q2_2014_State_of_Infection.pdf
11 https://www.politie.nl/nieuws/2015/april/13/11politie-zorgt-voor-doorbraak-in-recente-cryptoware-aanval.html
12 Bron: AIVD/MIVD.

Sony Pictures Entertainment hack

In november 2014 werd bekend dat er een omvangrijke digitale aanval op Sony plaatsvond. Hierbij is op grote schaal intellectueel eigendom en vertrouwelijke informatie buitgemaakt. Daarnaast is een aanzienlijk deel van de kantooromgeving gesaboteerd.

Deze aanvallen zijn opgeëist door de hackergroep Guardians of Peace (GOP). Deze groep eiste onder meer dat Sony The Interview intrekt, een film over een plot om de Noord-Koreaanse leider Kim Jong-un te vermoorden. De VS houdt Noord-Korea verantwoordelijk voor deze aanval.[13] Noord-Korea ontkent alle betrokkenheid.

Digitale aanval op TV5MONDE

Begin april 2015 is de Franse internationale televisiezender TV5MONDE slachtoffer geworden van een digitale aanval die afkomstig leek van een met ISIS sympathiserende hackersgroep 'CyberCaliphate'.[14] Deze groepering wordt ook verantwoordelijk gehouden voor de defacement van US CENTCOM (zie paragraaf Defacements op pagina 21). Door de aanval waren elf televisiekanalen, de Facebookpagina en de internetsite van de zender enkele uren niet beschikbaar. De aanval werd gezien als vergelding tegen Frankrijk voor hun deelname aan de strijd tegen ISIS.

Onderzoekers van beveiligingsbedrijf FireEye brachten twee maanden later naar buiten dat zij in de aanval het werk herkenden van een Russische hackergroep die bekend staat als APT28.[15] Volgens de onderzoekers zouden de hackers de jihadistische groepering als dekmantel gebruiken voor hun werkzaamheden. Dit voorbeeld toont aan hoe lastig de attributie van digitale aanvallen is.[16]

website Rijksoverheid.nl echter enkele uren onbereikbaar door een DDoS-aanval.[17] Ook de populaire weblog geenstijl.nl, die wordt gehost door hetzelfde bedrijf, werd door deze aanval getroffen.

De politie heeft in de rapportageperiode 67 aangiftes ontvangen van DDoS-aanvallen. De grote meerderheid van deze aangiftes werd gedaan door een organisatie.

Onderwijsinstellingen zijn regelmatig het slachtoffer van DDoS-aanvallen. Zo werd het ROC A12 meerdere keren getroffen door dit type aanvallen.[18] Ook scholen in Almere[19] en Winschoten[20] werden slachtoffer. Daar bleken eigen leerlingen de aanvallen te hebben uitgevoerd. Aangezien op veel scholen de rol van ICT in het onderwijsproces toeneemt, vormen dergelijke verstoringen voor docenten en studenten een groeiend probleem. Populaire Nederlandse sites, zoals nieuwssite nu.nl[21] en reisinformatiedienst 9292.nl,[22] ondervonden de afgelopen periode DDoS-aanvallen die hun beschikbaarheid verminderden. De daders en het motief van dergelijke aanvallen blijven meestal onbekend.

DDoS-aanvallen zijn een middel dat eenvoudig door actoren is in te zetten. Zelfs met weinig geld en kennis is een effectieve DDoS-aanval uit te voeren. Dit staat in schril contrast met de verstorende werking van de aanvallen. Als een dienst uren of dagen niet bereikbaar is, kan dit grote problemen met zich meebrengen.

De dreiging die uitgaat van DDoS-aanvallen verschilt onder organisaties binnen de overheid en de vitale sectoren in Nederland. Sommige organisaties hebben vrijwel continu te maken met DDoS-aanvallen (meerdere aanvallen per week), terwijl andere organisaties nog slechts sporadisch een aanval zien (enkele keren per jaar) of vrijwel niet meer te kampen hebben met deze problematiek. Het onderscheid in dreiging per sector blijkt ook uit het rapport State of the Internet Q1 2015 van Akamai.[23] Volgens dit rapport richten de meeste en zwaarste DDoS-aanvallen zich op bedrijven uit de spelindustrie (35,3 procent van de aanvallen) en de software/technologie-industrie (25,2 procent van de aanvallen), terwijl bijvoorbeeld overheidsinstellingen amper geraakt worden (1,8 procent van alle aanvallen). DDoS-aanvallen zijn hiermee echter niet slechts een probleem uit het verleden.

Wereldwijd is er een lichte stijging te zien in de intensiteit van DDoS-aanvallen. Begin 2015 werd bijvoorbeeld een Indiase netwerkprovider getroffen door een kortstondige aanval met een piek van 334 Gbps.[24] Dit was tot op dat moment de meest intensieve DDoS-aanval wereldwijd.

13 Bron: AIVD/MIVD.
14 http://www.ibtimes.com/french-tv-network-tv5monde-hit-pro-isis-cybercaliphate-hackers-1875314
15 http://www.buzzfeed.com/sheerafrenkel/experts-say-russians-may-have-posed-as-isis-to-hack-french-t#.hkaK8DKGK
16 Zie ook: Hoofdstuk 2, Actoren.
17 https://www.security.nl/posting/418103/Storing+Rijksoverheid_nl+veroorzaakt+door+DDoS-aanval
18 http://www.gelderlander.nl/regio/de-vallei/ede/opnieuw-cyberaanval-op-netwerk-roc-a12-1.4791497?ls=pl
19 http://www.omroepflevoland.nl/nieuws/121705/almere-leerlingen-leggen-computersysteem-plat
20 http://nis.rtvnoord.com/artikel/artikel.asp?p=141973
21 http://www.automatiseringgids.nl/nieuws/2015/08/nu.nl-plat-door-ddos-aanval
22 http://tweakers.net/nieuws/95475/reissite-9292-kampt-al-een-dag-met-ddos-aanval.html
23 http://www.stateoftheinternet.com/downloads/pdfs/2015-internet-security-report-q1.pdf
24 http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5405-arbor-networks-records-largest-ever-ddos-attack-in-q1-2015-ddos-report

GitHub is een populaire site waarop opensourcesoftware in samenwerkingsprojecten wordt ontwikkeld en verspreid. In maart 2015 kreeg de site een omvangrijke DDoS-aanval vanaf Chinese IP-adressen te verwerken.[25] Deze aanval werd deels gerouteerd via Nederlandse ICT-infrastructuur.[26] De aanvallen waren gericht op twee ontwikkelingsprojecten van software, bedoeld voor het omzeilen van Chinese censuurmaatregelen.

Toen begin 2015, kort na de aanslag op het satirische Franse tijdschrift Charlie Hebdo in Frankrijk, 19.000 websites offline gingen werd al snel gedacht aan een DDoS-aanval vanuit jihadistische hoek.[27] Na enkele dagen bleek echter een menselijke fout bij hostingprovider Oxalide[28] de oorzaak te zijn.

Defacements

Dagelijks worden wereldwijd honderden websites getroffen door een defacement; ook in Nederland zijn dit elke dag tientallen websites.[29] In bijna alle gevallen komt dit door zogenaamde mass defacements, waarbij grote hoeveelheden webservers worden gescand op zoek naar kwetsbaarheden. Bij een ontdekte kwetsbaarheid plaatst de aanvaller vervolgens opvallend een boodschap op de website met de melding dat deze gehackt is. In veel gevallen is dit een ideologische boodschap. Ook vinden er gerichte defacements plaats, waarbij de betrokken organisatie voor de aanvaller een ideologische of politieke lading heeft. Dergelijke gerichte aanvallen hebben het afgelopen jaar voor zover bekend echter niet plaatsgevonden op Nederlandse sites.

De aanslag op Charlie Hebdo werd gevolgd door defacements van vooral Franse websites. De eerder genoemde Anonymous-actie #OpCharlieHebdo leidde tot een tegenactie #OpFrance.[30] Hierbij werden tientallen Franse websites voorzien van voorpagina's met islamitische teksten.

De pro-Palestijnse hackers van AnonGhost waren de afgelopen periode buitengewoon actief met defacements. Websites van de Verenigde Naties[31] en diverse Israëlische organisaties[32], maar bijvoorbeeld ook van Air France[33] en American Express[34], werden voorzien van ideologische boodschappen.

Een ander populair type defacement is het kapen van accounts op sociale media. Aanvallers achterhalen inloggegevens, bijvoorbeeld met behulp van phishing. De gevolgen voor de informatiebeveiliging van de organisatie zijn beperkt, omdat de aanvallers niet het netwerk van de organisatie aanvallen. De reputatieschade kan echter aanzienlijk zijn. Dit type aanval is vooral populair onder ideologisch gemotiveerde aanvallers.

De burgeroorlog in Syrië en de opkomst van ISIS zijn aanleiding geweest voor diverse defacementcampagnes gericht tegen westerse websites en sociale media. De hack op Twitter- en YouTube-accounts van US Central Command, de Amerikaanse legermacht voor het Midden-Oosten en Zuid-Azië, sprong het meest in het oog. Het profiel bevatte een foto van een gemaskerde militant en opschriften als 'Cybercaliphate' en 'I love you ISIS'.[35]

Ook jihadistische sociale media lagen onder vuur. Medio 2014 lanceerde Anonymous de operatie #OpIceISIS met als doel ideologische uitingen van ISIS, onder andere via Twitter-accounts van sympathisanten, te bestrijden.[36]

Malwarebesmettingen

Gehackte websites kunnen voor de verspreiding van grote hoeveelheden malware zorgen. Een onderzoek[37] naar de kwetsbaarheid van de wereldwijd meest bezochte websites had als uitkomst dat 6 procent van deze websites malware of spam verspreidde of onderdeel was van een botnet. 21 procent van de sites draaide op software met bekende kwetsbaarheden. Dit waren vooral kwetsbaarheden in veelgebruikte componenten zoals PHP, IIS en Apache, maar ook in CMS-software als Drupal of WordPress. Volgens hetzelfde onderzoek zou 99 procent van alle malwarebesmettingen worden opgelopen door het bezoeken van websites.

De mate waarin Nederlandse computers geconfronteerd worden met malware, is al enkele jaren stabiel.[38] In het derde en vierde kwartaal van 2014 kreeg respectievelijk 13,8 procent en 10,1 procent van de Nederlandse Windowscomputers te maken met malware, bijvoorbeeld door het bezoeken van een website die malware probeerde te installeren (wereldwijd: 20,1 procent en 15,9 procent).[39]

25 http://www.networkworld.com/article/2903317/microsoft-subnet/largest-ddos-attack-in-githubs-history-targets-anticensorship-projects.html
26 https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1
27 http://www.volkskrant.nl/aanslag-op-charlie-hebdo/franse-sites-gehackt-in-digitale-jihad-oorlog~a3830794/
28 http://www.silicon.fr/indisponibilite-oxalide-erreur-humaine-non-attaque-106435.html
29 Bron: eigen telling op basis van meldingen op zone-h.org.
30 https://www.mashable.com/2015/01/13/islamist-hackers-french-sites-anonymous/
31 http://www.ibtimes.co.uk/anonghost-hackers-deface-un-website-following-al-asqa-mosque-tensions-1474258
32 http://www.theprohackers.com/2014/04/opisrael-anonghost-hacked-2000-websites.html
33 http://www.batblue.com/anonghost-hacks-air-france-website/
34 http://cyberwarzone.com/breaking-news-subdomain-american-express-website-hacked-anonghost/
35 http://techcrunch.com/2015/01/12/cyber-caliphate/
36 http://www.hackersnewsbulletin.com/2014/09/anonymous-hackers-launch-cyber-war-isis.html
37 https://www.menlosecurity.com/resources/Menlo_Security_Vulnerability_Report_Mar_2015.pdf
38 Bron: vergelijking van de recentste Microsoft Security Intelligence Reports (https://microsoft.com/sir).
39 Bron: https://microsoft.com/sir.

De meeste confrontaties leidden echter niet tot een infectie. Als Nederlandse computergebruikers bijvoorbeeld de Malicious Software Removal Tool van Microsoft gebruikten, werd er in deze periodes slechts in 3,4‰ en 1,9‰ van de gevallen malware aangetroffen en verwijderd.

Besmetting door advertentiesites

De afgelopen rapportageperiode werden zowel nationaal als internationaal advertentieservers misbruikt voor het verspreiden van malware. In Nederland werden veelbezochte sites als nu.nl,[40] telegraaf.nl, prive.nl[41] en weer.nl slachtoffer van zogenaamde malvertising.

Advertentieleveranciers van Google werden meerdere keren getroffen door dergelijke aanvallen. In 2014 was Googles advertentieservice DoubleClick meerdere malen de verspreider van malwarebesmettingen. In april 2015 werden bezoekers via een Bulgaarse partner Engage Lab gedurende enkele uren ongemerkt naar een site gestuurd, waar de Nuclear Exploit Kit zocht naar kwetsbaarheden in hun systeem om daar vervolgens malware te installeren.[42]

In 2014 plaatste een aanvaller besmette advertenties op sites die de interesse van zijn doelgroep hadden. Hij deed dit met behulp van online advertentieveilingen. Zo kon hij gericht systemen binnendringen. De campagne leek zich vooral te richten op de Amerikaanse defensie-industrie. Door het bedrijf dat de campagne ontdekte werd deze aanval Operation Deathclick[43] genoemd.

Uitval ICT

Storingen zonder moedwillige dader kunnen zorgen voor een verlaging van de beschikbaarheid van diensten. Verstoringen van dit type kunnen minstens zulke grote gevolgen hebben als moedwillige verstoringen.

Eind maart 2015 werden Noord-Holland en Flevoland getroffen door een aanzienlijke stroomstoring.[44] Ondanks overlast door vastgelopen metro's en liften en uitval van het treinverkeer, bleven grote ICT-storingen door de stroomuitval beperkt. Belangrijke rekencentra in het getroffen gebied konden de uitvalperiode op hun noodstroomvoorziening doorkomen.

Digitale spionage

Waar voorgaande manifestaties vooral gericht waren op de ICT, is bij spionage het verkrijgen van informatie het doel.

Het aantal digitale spionageaanvallen richting Nederland die een dreiging voor de nationale veiligheid en economische belangen vormen, is het afgelopen jaar fors toegenomen. Uit onderzoek van de AIVD en de MIVD is gebleken dat Nederlandse overheidsinstellingen in 2014 veelvuldig doelwit zijn geweest van geavanceerde digitale spionageaanvallen. Het merendeel van deze aanvallen is uitgevoerd met spearphishing-e-mails die met malware besmette bijlagen of links naar websites met malware bevatten.

Daarnaast zijn Nederlandse overheidsinstanties en bedrijven, waaronder defensiegerelateerde bedrijven, slachtoffer geweest van zogenaamde wateringhole-aanvallen waarbij malware op gerichte websites wordt geplaatst om bezoekers te besmetten. Deze aanvallen tonen aan dat Nederlandse overheidsinstellingen en bedrijven structureel doelwit zijn van digitale spionage. Gezien de wereldwijde omvang en toename van digitale spionage betreft het aantal waargenomen incidenten vermoedelijk slechts een fractie van het daadwerkelijke aantal. Hierdoor is het aannemelijk dat de omvang van digitale spionage in Nederland groter is dan nu wordt waargenomen.[45] Het valt niet te verwachten dat er beter en eerder zicht te krijgen is op dergelijke activiteiten zonder de bredere inzet van host-based defence, anomaliedetectie en patroonherkenning.

Het in Nederland gevestigde Franse bedrijf Gemalto bevestigde begin 2015 dat zij in de periode 2010 en 2011 slachtoffer zijn geworden van digitale spionageaanvallen.[46] Hierbij is getracht sleutelmateriaal van simkaarten te onderscheppen. De aanval, die volgens Gemalto waarschijnlijk is uitgevoerd door het Britse GCHQ en de Amerikaanse NSA, raakte alleen kantoornetwerken en kan volgens het bedrijf niet hebben geleid tot grootschalige diefstal van encryptiesleutels van simkaarten.[46] De AIVD heeft naar aanleiding van de berichtgeving in de media een feitenonderzoek uitgevoerd naar de vermeende Gemalto-hack. Over de uitkomst van dit onderzoek zijn de belangendragers via de geëigende kanalen geïnformeerd.

Ook in het buitenland werd een aantal digitale spionagezaken bekend. In mei 2014 kwam in het nieuws dat de Belgische Federale Overheidsdienst Buitenlandse Zaken was gehackt.[47] Naar verluidt Russische hackers trachtten geheime NAVO-documenten over de

40 http://tweakers.net/nieuws/97041/nu-punt-nl-verspreidde-malware-via-geinfecteerd-advertentienetwerk-update-2.html
41 https://www.security.nl/posting/389362/Advertenties+op+Telegraaf,+Priv%C3%A9+en+Vl+verspreiden+malware
42 http://blog.fox-it.com/2015/04/07/liveblog-malvertising-from-google-advertisements-via-possibly-compromised-reseller/
43 http://www.invincea.com/2014/10/webinar-targeted-malvertising/
44 http://www.nrc.nl/nieuws/2015/03/27/dit-zijn-de-gevolgen-van-de-grote-stroomstoring-in-noord-holland/
45 Bron: AIVD/MIVD.
46 http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx
47 http://www.tijd.be/nieuws/politiek_economie_belgie/Moskou_hackt_Belgische_staat.9499843-3136.art

Digitale oorlogsvoering[49]

De afgelopen periode is wereldwijd, net als voorgaande jaren, fors geïnvesteerd in (offensieve) digitale capaciteit en de bijbehorende inzetmiddelen. Desondanks zijn er geen voorbeelden hiervan in klassieke militaire zin. Hierbij zijn er enerzijds dodelijke slachtoffers of vernietiging toe te schrijven aan de inzetmiddelen en anderzijds zijn er activiteiten ontplooid die zich richtten op het breed verstoren, veranderen, misleiden of vernietigen van een tegenstander in een gewapend conflict. Er is dan ook geen sprake geweest van zuiver digitale oorlogvoering. Mogelijke oorzaken hiervoor zijn onvoorziene neveneffecten die op kunnen treden bij het gebruik van dergelijke digitale inzetmiddelen en het feit dat dergelijke technisch complexe aanvallen gespecialiseerde kennis en een technisch hoogwaardige infrastructuur vereisen. De opbouw van dergelijke kennis en infrastructuur kost veel tijd. Daarnaast is het zo dat ondanks de toename van offensieve cybercapaciteiten, de daadwerkelijke inzet significante juridische, politieke en morele implicaties met zich meebrengt.

Desondanks zijn wel degelijk een groeiend aantal cyberoperaties en digitale aanvallen met een politiek-militair doel waargenomen. Deze vormden echter een onderdeel van zogenoemde hybride oorlogvoering. Bij hybride oorlogvoering wordt gebruik gemaakt van combinaties van alle mogelijke middelen (waaronder politieke, economische en/of militaire middelen inclusief cybercapaciteit) die op de situatie worden toegespitst om maximaal rendement te behalen tegen minimale kosten. Dit rendement is over het algemeen een door de politieke leiding gesteld doel. Door (delen van) de middelen heimelijk in te zetten wordt het mogelijk de verantwoordelijkheid voor de activiteiten te ontkennen of de (schijn van) verantwoordelijkheid bij een derde partij te leggen. Dit concept is niet nieuw, maar de toevoeging van cyberoperaties maakt het onderwerp relevant.

Voorbeelden van cyberoperaties (al dan niet heimelijk of afgeschermd) die passen binnen hybride oorlogsvoering zijn de ruim honderd DDoS-aanvallen die door pro-Russische hackers zijn uitgevoerd op Oekraïense websites met een pro-Europese signatuur. Ook is de NAVO, voorafgaand aan of tijdens bijeenkomsten over de crisis in Oekraïne, meerdere keren slachtoffer geworden van dit soort aanvallen. Verder hebben pro-Russische hackers daags voor een ontmoeting tussen de Oekraïense premier en de Duitse bondskanselier DDoS-aanvallen uitgevoerd op de websites van de bondskanselier en de Bondsdag.

Activiteiten die samenhangen met hybride oorlogvoering beperken zich niet alleen tot crisisgebieden. Zo zijn er in het Westen in het digitale domein enkele coherente, waarschijnlijk door staten uitgevoerde of gesponsorde pogingen waargenomen om industriële controlesystemen in kaart te brengen (spionage) en te prepareren voor sabotage. De stap van digitale spionage naar digitale of hybride oorlogvoering is dan klein. Zodra toegang verkregen is tot dergelijke systemen en er informatie kan worden onttrokken, is het eenvoudig om fysieke effecten te bewerkstellingen aan of met de systemen. Bij een militair conflict of spanningen over belangenbehartiging tussen staten, kan deze kennis of toegang op termijn gebruikt worden voor militaire doeleinden of sabotage. Vooral door attributieproblemen en de potentiële impact van cyberoperaties op de maatschappij is dit een zorgelijke (politiek-militaire) ontwikkeling.

Oekraïne-crisis buit te maken met behulp van het Snake-virus. Belgische media berichtten dat de Amerikaanse CIA de Belgische inlichtingendienst attendeerde op de hack.[49] In oktober 2014 werd een hack op het netwerk van het Witte Huis ontdekt. Het zou gaan om het niet-geclassificeerde netwerk van de Executive Office of the President.[50]

Economische spionage

De AIVD en de MIVD hebben het afgelopen jaar meerdere digitale spionageaanvallen onderkend die twintig Nederlandse bedrijven als doelwit hadden. Hoogstwaarschijnlijk waren deze afkomstig van buitenlandse inlichtingendiensten.[51] Deze bedrijven zijn voornamelijk actief binnen de defensie-, hightech-, tuinbouw-, chemie-, energie- en ruimte- en luchtvaartsector. Aangezien bedrijven niet verplicht zijn dergelijke aanvallen te melden, is de totale omvang van deze digitale spionageaanvallen op Nederlandse bedrijven en de economische schade als gevolg hiervan moeilijk vast te stellen.

Er zijn ook voorbeelden bekend van spionageaanvallen op ICS en van malware die specifiek gericht is op de verkenning van ICS.[52] Dergelijke malware is ook aangetroffen bij Nederlandse bedrijven.[53]

De Nederlandse chipmachinefabrikant ASML heeft in een persbericht[54] verklaard dat er is ingebroken op de ICT-systemen van het

48 Bron: MIVD.
49 http://www.standaard.be/cnt/dmf20140514_01105038
50 http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html
51 Bron: AIVD/MIVD.
52 Voorbeelden hiervan zijn Black Energy en HAVEX.
53 Bron: AIVD/MIVD.
54 http://www.asml.com/asml/show.do?lang=EN&ctx=5869&rid=51584

bedrijf. Hierdoor hadden derden een korte periode toegang tot een beperkt deel van de ICT-systemen. Er is volgens ASML geen ongeautoriseerde toegang tot waardevolle informatie van het bedrijf, zijn klanten of toeleveranciers vastgesteld. Het is onbekend wie verantwoordelijk is voor de digitale aanval.

Diefstal van informatie

Hoewel ook bij spionage sprake is van het ontvreemden van vertrouwelijke informatie, wordt gesproken van diefstal van informatie wanneer aanvallers data stelen met als doel deze met winstoogmerk te verkopen, te publiceren of voor activistische doeleinden te misbruiken.

Incidenten in de gezondheidszorg

Een nieuwe ontwikkeling in de afgelopen periode was de sterke stijging in het aantal datadiefstallen gericht op patiëntinformatie. Vooral in de Verenigde Staten waren ziektekostenverzekeraars en medische instellingen een gewild doelwit. Volgens Dell SecureWorks werden patiëntgegevens op ondergrondse marktplaatsen in 2013 verkocht voor 20 dollar per stuk.[55] Dit was toen al 10 tot 20 keer zo veel als de prijs van een creditcardnummer met veiligheidscode.

Bij diefstal van persoonsgegevens bij Community Health Systems[56] (4,5 miljoen patiënten), Anthem[57] (80 miljoen verzekerden) en Premera[58] (11 miljoen verzekerden) werd in alle gevallen de link gelegd naar Chinese daders. Harde bewijzen zijn hiervoor echter niet naar buiten gebracht. Hierdoor is het onduidelijk wat de intentie van de daders is: spionage of diefstal.

Gezien de hoeveelheid geld die ook in Nederland in deze sector wordt omgezet, worden dergelijke gegevens mogelijk een aantrekkelijk doelwit. Desondanks is in Nederland geen grote diefstal van medische gegevens ontdekt.

Het Amerikaanse beveiligingsbedrijf Hold Security kreeg in 2014 een dataset in handen bestaande uit 4,5 miljard gestolen gebruikersnamen en wachtwoorden. Deze waren afkomstig van circa 400.000 kwetsbare websites. Nadat het NCSC de beschikking had gekregen over de set met kwetsbare websites en gestolen e-mailadressen uit het .nl-domein, konden getroffen partijen geïnformeerd worden.[59] Ook de Duitse overheid kreeg in april 2014 een dataset met 18 miljoen door cybercriminelen bemachtigde inloggegevens. In samenwerking met het NCSC zette de Duitse BSI een site[60] op waar gebruikers konden controleren of hun e-mailadres onderdeel uitmaakte van de dataset.

In april 2015 meldde webwinkel mapp.nl dat door SQL-injectie 157.000 e-mailadressen en gehashte wachtwoorden[61] waren ontvreemd. De webwinkel heeft alle wachtwoorden gereset en haar klanten geïnformeerd over de datadiefstal.

Onderzoekscentrum Ponemon Institute kenmerkte 2014 als Year of the Mega Breaches[62] vanwege de hoeveelheid datalekken met grote aantallen slachtoffers. Vooral in de VS werden de kassasystemen (Point-of-Sale, PoS) van grote winkelketens getroffen door gegevensdiefstallen.

Bij Home Depot betrof dit gegevens over 56 miljoen betaalpassen en creditcards plus 53 miljoen e-mailadressen van klanten. Andere grote datadiefstallen waarbij informatie van betaalkaarten werd buitgemaakt betroffen Staples[63] (1,1 miljoen betaalkaarten) en Michaels Arts & Crafts[64] (3 miljoen betaalkaarten). Door de chip in Nederlandse betaalpassen levert het verzamelen van gegevens van betaalkaarten hier voor criminelen weinig op.

In juli 2014 ontdekte de Amerikaanse bank JPMorgan Chase een serieuze datadiefstal. De diefstal betrof namen en huis- en e-mailadressen van in totaal 76 miljoen huishoudens en 6 miljoen kleine bedrijven.[65] Rekeningnummers en wachtwoorden zijn niet buitgemaakt. De inbraak bleek mogelijk doordat men op één testsysteem vergeten was de tweefactorauthenticatie te activeren.[66] Bij een digitale inbraak bij online veilingsite eBay in mei 2014 werden gegevens van een onbekend aantal gebruikers gestolen.[67] Uit voorzorg verzocht eBay alle 145 miljoen gebruikers hun wachtwoord te wijzigen.

55 http://www.secureworks.com/resources/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents/
56 http://www.informationweek.com/attacks-breaches/chinese-hackers-hit-community-health-system/d/d-id/1298099
57 http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack
58 http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/
59 https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-verkrijgt-nederlandse-gegevens-van-hold-security.html
60 https://www.ncsc.nl/actueel/nieuwsberichten/nederlandse-accountgegevens-buitgemaakt-in-duitsland.html
61 https://www.security.nl/posting/425241/Gegevens+157_000+klanten+Mapp_nl+gestolen
62 http://www.ponemon.org/library/2014-a-year-of-mega-breaches
63 https://threatpost.com/staples-confirms-1-2-million-cards-lost-in-breach/110030
64 http://krebsonsecurity.com/2014/04/3-million-customer-credit-debit-cards-stolen-in-michaels-aaron-brothers-breaches/
65 http://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach
66 http://www.esecurityplanet.com/network-security/entry-point-identified-for-jpmorgan-chase-breach.html
67 http://www.cnet.com/news/ebay-hacked-requests-all-users-change-passwords/

De diefstal en publicatie vanuit iCloud van naaktfoto's van diverse beroemdheden,[68] ook wel bekend als the Fappening, leidde vorig jaar tot veel ophef. Toen vervolgens ook bijna 100.000 Snapchat-foto's werden gelekt vanuit de third-party app SnapSaved, werd dit direct bekend als the Snappening.[69] Deze incidenten brachten het gevaar van foto's opslaan of delen via de cloud zonder expliciete aandacht voor de beveiliging wereldwijd onder de aandacht.

Diefstal van financiële middelen

Informatie is geld waard. Daarom trachten criminelen datasets te bemachtigen en vervolgens voor veel geld te verkopen. Er is een methode die nog sneller werkt, namelijk het stelen van geld door het inzetten van malware.

Diefstal door malware op geldautomaten vond de afgelopen periode ook in West-Europa plaats.[70] Deze vorm van diefstal was hier eerder nog niet waargenomen. Criminelen installeren eerst malware op een geldautomaat; hiervoor is fysieke toegang tot het apparaat noodzakelijk. Daarna kunnen zij de automaten leeghalen na het invoeren van een bepaalde code.

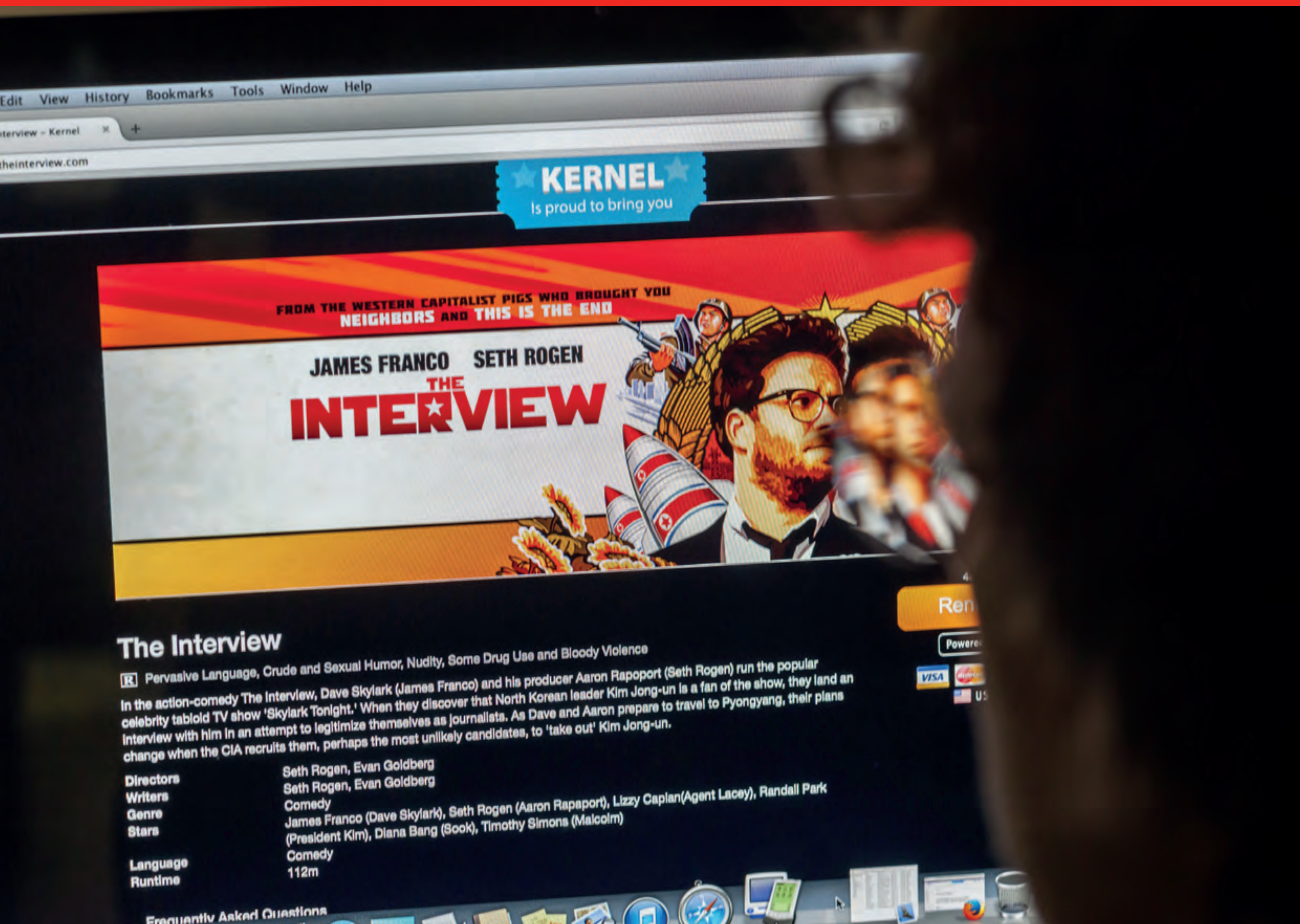
Een grotere slag sloegen de criminelen die achter de Carbanak- of Anunak-campagne zaten. Beveiligingsbedrijven Fox-IT[71] en Kaspersky[72] publiceerden hierover. De Carbanak-bende wist door gebruik van spearphishing-e-mails meerdere banken te besmetten en deed daarna langdurig onderzoek naar de werkwijze van de verschillende banken. Vervolgens werd er op diverse manieren geld buitgemaakt, onder andere door geld over te maken naar eigen rekeningen en door geldautomaten te manipuleren. Schattingen van de opbrengst van deze bende liggen tussen 250 miljoen en 1 miljard dollar. Nederlandse banken hebben aangegeven geen slachtoffer te zijn van Carbanak.

Aanvallen op klanten van Nederlandse banken waren de laatste tijd minder succesvol dan in eerdere jaren. De schade door phishing op klanten van Nederlandse banken is afgenomen tot 3,9 miljoen euro in 2014 tegen 4,7 miljoen euro een jaar eerder.[73] Deze dalende trend houdt al enkele jaren aan. Ook geven de banken aan dat schade door malware in deze periode met 90% is gedaald.

Daarnaast werden de afgelopen periode ook diverse bitcoin-diefstallen uitgevoerd. In januari 2015 werd bij de Europese bitcoinbeurs Bitstamp bijna 19.000 bitcoin (ruim 4 miljoen euro) gestolen.[74] Daarnaast vonden diverse kleinere diefstallen van bitcoins[75] en andere cryptocurrency's[76] plaats. Na het faillissement van de grote bitcoinbeurs Mt. Gox begin 2014, waarbij ongeveer 850.000 bitcoin verdween, is de koers van de bitcoin continu gedaald.

68 http://www.ibtimes.com/jennifer-lawrence-victoria-justice-apparent-nude-photos-leaked-twitter-1674758
69 http://www.ibtimes.com/snappening-how-much-trouble-leaked-snapchat-photos-can-get-you-1704287
70 https://www.security.nl/posting/405528/Malware+op+20+geldautomaten+in+West-Europa+ontdekt
71 https://www.fox-it.com/en/press-releases/anunak/
72 https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/
73 http://www.betaalvereniging.nl/wp-uploads/2015/03/150318-Fraude-betalingsverkeer-gehalveerd-20141.pdf
74 http://www.zdnet.com/article/bitstamp-bitcoin-exchange-suspended-amid-hack-concerns-heres-what-we-know/
75 http://www.coindesk.com/bitcoin-firm-coinapult-restores-services-following-hack/ en https://www.cryptocoinsnews.com/allcrypt-com-bitcoin-exchange-goes/
76 https://www.cryptocoinsnews.com/bitcoin-altcoin-exchange-cryptoine-hacked/

Het is voor een crimineel al lang niet meer nodig om digitale vaardigheden te bezitten om gebruik te kunnen maken van digitale aanvallen.



2 Dreigingen: Actoren

De grootste dreiging gaat net als vorige jaren uit van beroepscriminelen en statelijke actoren. Hun aantallen nemen toe, evenals hun capaciteiten. Hoewel de potentie op digitaal gebied van terroristische actoren groeiende is, vormen ze nog geen grote dreiging vanwege hun beperkte technische capaciteiten.

Dit hoofdstuk gaat in op actoren die de betrouwbaarheid en de beveiliging van informatie(systemen) aantasten, hun capaciteiten en ontwikkelingen op dit vlak.

Beroepscriminelen

De intentie van beroepscriminelen is het verdienen van geld. Criminelen ontwikkelen hun digitale vaardigheden steeds verder. De werkwijze van criminelen verandert voortdurend en is innovatief. Het afgelopen jaar vielen enkele digitale aanvallen door criminelen op door de goede organisatie, nauwkeurige uitvoering en technische geavanceerdheid.[77 78 79] Cybercriminaliteit kent een hoge mate van geografische spreiding, zowel van de daders en slachtoffers als van hun infrastructuur. Deze geografische spreiding maakt internationale samenwerking noodzakelijk. De dreiging die uitgaat van zowel vernieuwende als traditionele aanvallen van criminelen neemt toe.

Dit jaar viel vooral op dat cybercriminelen bereid zijn om veel tijd te investeren in de voorbereiding van digitale aanvallen. Dit was bijvoorbeeld te zien bij Carbanak, een geavanceerde aanval op Oost-Europese banken. Via malware konden criminelen de activiteiten van bankmedewerkers een lange tijd digitaal observeren, zodat de criminelen uiteindelijk grote sommen geld naar bankrekeningen konden overmaken en geldmachines konden manipuleren.[80]

Niet alleen tonen cybercriminelen meer geduld in de uitvoering van hun activiteiten en zijn zij goed georganiseerd, ook worden zij creatiever met het verzilveren van gestolen gegevens. In de Verenigde Staten onttrokken aanvallers met een zeer gerichte malwarecampagne beursgevoelige informatie uit de farmaceutische sector. Op basis van deze informatie was het mogelijk om koersen te voorspellen.[81]

Een ander type aanval door criminelen dat afgelopen jaar sterk in opkomst was, is het gebruik van Point-of-Sale-malware, dat zich richt op verkooppunten.[82] Voor Nederland lijkt deze zogenoemde PoS-malware geen grote dreiging te vormen, voornamelijk omdat Nederlandse pinpassen zijn uitgerust met EMV-technologie, een chip die het kopiëren van informatie op de chip bemoeilijkt. Ook beschermen betaalautomaten gelezen kaartdata direct tegen kopiëren.

Hiernaast richten criminelen in de Verenigde Staten zich steeds meer op datadiefstallen in de medische sector.[83 84 85] Vaak gaat het om patiëntgegevens van zorgverzekeraars. Vermoedelijk is het de aanvallers bij deze hacks te doen om de burgerservicenummers, geboortedata en medische informatie. Hiermee kan de aanvaller

77 https://www.fox-it.com/en/press-releases/anunak/
78 http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide
79 http://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf
80 https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
81 http://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf
82 In Hoofdstuk 1 is al ingegaan op dit type aanvallen.
83 http://abcnews.go.com/Business/fbi-investigating-cyberattack-health-insurance-company-affect-11/story?id=29705722
84 http://www.ehackingnews.com/2015/03/data-breach-at-sacred-heart-health.htmlv
85 http://www.databreaches.net/childrens-national-health-system-notified-18000-patients-after-employees-fell-for-phishing-scheme/

niet alleen financiële fraude plegen, maar ook zorgverzekeringsfraude.[86] Deze aanvallen zijn nog niet in Nederland waargenomen.

Naast deze ontwikkelingen houden criminelen zich nog steeds bezig met minder gerichte aanvallen, zoals de inzet van cryptoware, phishing en afpersing met DDoS-aanvallen. Ook leveren criminelen diensten op maat aan andere partijen. Deze zogenoemde 'cybercrime-as-a-service' blijft zich verder ontwikkelen en professionaliseren. Deze diensten zijn zo omvangrijk geworden dat zij op de ondergrondse markt zelfs aan concurrentie onderhevig zijn. Dit dwingt deze diensten ook om steeds betrouwbaarder te worden voor de afnemer.[87]

Een crimineel heeft al lang geen digitale vaardigheden meer nodig om digitale aanvallen uit te voeren. Het is daarom voorstelbaar dat het aantal digitale aanvallen door criminelen niet alleen in omvang, maar ook in diversiteit zal toenemen.[88]

Interactie tussen actoren bemoeilijkt attributie

De interactie tussen statelijke actoren, criminelen en hacktivisten wordt steeds intensiever.[89] Hulpmiddelen die tot nu toe het meest door statelijke actoren gebruikt werden, zijn op de ondergrondse markt vrij verkrijgbaar en beschikbaar geworden voor andere groepen actoren, zoals criminelen. Ook komt het voor dat statelijke actoren hulpmiddelen gebruiken die eerder alleen voor andere typen aanvallen werden gebruikt. Het afgelopen jaar werd bijvoorbeeld specifieke malware ingezet voor spionageaanvallen op bedrijven en instellingen uit Oekraïne, die eerder geassocieerd werd met aanvallen van criminele aard.[90 91]

Hacktivisten en ideologische/patriottische hackers kunnen activiteiten ontplooien die in lijn lijken met de belangen van een staat. Het is bij deze activiteiten dan moeilijk aan het motief af te leiden van welke soort actor de aanval afkomstig is. Staten kunnen ook de samenwerking opzoeken met hacktivisten en kunnen hacktivisten inhuren voor hun eigen doeleinden. Deze banden zijn vaak moeilijk aan te tonen.

Door diverse technische moeilijkheden is attributie van digitale aanvallen altijd een lastige aangelegenheid geweest. De aanvallen op Sony Pictures Entertainment en de Franse TV zender TV5MONDE zoals beschreven in hoofdstuk 1, zijn hier een goed voorbeeld van. De interactie tussen groepen actoren bemoeilijkt de analyse van aanvallen en groepen digitale actoren des te meer.

Statelijke actoren

De Nederlandse nationale veiligheid en economie worden bedreigd door statelijke actoren. Digitale aanvallen zijn een aantrekkelijk alternatief voor conventionele militaire en spionagemiddelen vanwege de grote omvang en impact tegen lage kosten en afbreukrisico's. Hierdoor neemt het aantal actoren dat een potentiële dreiging kan vormen voor de Nederlandse nationale veiligheid toe.[92]

In de rapportageperiode is een toename waargenomen van het aantal landen dat digitale aanvallen op of via de infrastructuur van Nederlandse organisaties uitvoert.[92] In het merendeel van de gevallen betreft het digitale spionage, waaronder steeds meer economische spionage. Daarnaast waren er enkele gevallen van misbruik van Nederlandse infrastructuur voor digitale sabotageaanvallen op organisaties buiten Nederland.

De grootste digitale spionagedreiging komt van buitenlandse inlichtingendiensten. Daarnaast is de omvang en diversiteit van betrokken actoren toegenomen. Buitenlandse inlichtingendiensten maken voor digitale aanvallen vaak gebruik van de aanwezige kennis, capaciteit en middelen bij hackers en private organisaties, zoals ICT-bedrijven en universiteiten. Vaak wordt de software of infrastructuur van deze organisaties ingezet voor spionage.[92]

Verder hebben actoren met een niet-democratische of autoritaire achtergrond in het digitale domein een groot voordeel. Ondanks de internationale consensus dat de internationale rechtsorde ook in cyberspace van toepassing is, laten deze actoren zich ook minder gelegen liggen aan het naleven hiervan. Zij zijn in staat hun technologisch gezien wellicht mindere capaciteit flexibel en uiterst effectief in te zetten, omdat er geen sprake is van onafhankelijk toezicht en noodzaak tot transparantie. Private groeperingen kunnen in dergelijke landen vaak ongestoord hun activiteiten ontplooien, omdat ze een vorm van bescherming genieten binnen verschillende lagen van de overheid en er zelfs sprake kan zijn van symbiotisch optreden. Deze toename van het aantal betrokken actoren bemoeilijkt een betrouwbare attributie van aanvallen.

Terroristen

Het doel van terroristen is het teweegbrengen van politiek-ideologische veranderingen door het creëren van angst. Hoewel de potentie op digitaal gebied van terroristische actoren groeiende is,[93] vormen ze nog geen grote dreiging vanwege hun beperkte

86 http://www.secureworks.com/resources/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents/
87 https://blogs.rsa.com/cybercrime-2015-inside-look-changing-threat-landscape/
88 https://www.aivd.nl/@3247/jaarverslag-aivd/
89 https://www2.fireeye.com/WEB-2015RPTM-Trends.html
90 https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf
91 https://www2.fireeye.com/WEB-2015RPTM-Trends.html
92 Bron: AIVD/MIVD.
93 https://www.aivd.nl/@3247/jaarverslag-aivd/

technische capaciteiten. Er zijn geen aanwijzingen die wijzen op een concrete dreiging richting Nederland.[94]

In het kader van digitale aanvallen door terroristen gaat de grootste dreiging op dit moment uit van het jihadisme.[95] Met de opkomst van jihadistische groeperingen zoals ISIS, heeft de media volop aandacht voor de digitale activiteiten van jihadistische groeperingen of jihadistische sympathisanten. Ook hebben jihadistische groeperingen herhaaldelijk opgeroepen tot het voeren van een digitale oorlog of een 'cyber-jihad' tegen het Westen.[96][97] Deze ontwikkelingen riepen de afgelopen jaren de vraag op in hoeverre jihadistische actoren de capaciteiten hebben om digitale aanvallen te plegen die de maatschappij ontwrichten.

Tot nu toe zijn digitale aanvallen met jihadistische motieven in Nederland beperkt gebleven tot kleinschalige aanvallen waar weinig kennis en mankracht voor nodig was. Het gaat hier voornamelijk om defacements van websites en DDoS-aanvallen.[98] Het motief van deze aanvallen lijkt vooralsnog het verspreiden van propaganda.

Capaciteiten van terroristen

In het buitenland is te zien dat jihadisten gebruik beginnen te maken van laagdrempelige malware. In Syrië zijn digitale aanvallen waargenomen waarvan wordt vermoed dat deze door ISIS uitgevoerd zijn om op lokaal niveau locatiegegevens van doelwitten te bepalen.[99]

Jihadistische groeperingen plaatsen informatie en instructievideo's op het internet om digitale vaardigheden van aanhangers verder te verspreiden.[100] Deze instructies zijn met name gericht op het digitaal veiligheidsbewustzijn van aspirant-jihadisten.[101][102] Ook zijn er instructies aangetroffen voor het gebruik van een Remote Acces Tool (RAT).[103] Hoewel het gebruik van RAT's door jihadistische groeperingen in Nederland en in het buitenland nog niet is waargenomen, is het gebruik ervan inmiddels wijdverspreid onder verschillende politieke facties in het Midden-Oosten.[104] Door deze ontwikkelingen is het voorstelbaar dat de digitale capaciteiten van jihadistische groeperingen in de toekomst verder toenemen en dat zij deze activiteiten ook tegen Nederlandse belangen kunnen inzetten.

Jihadistische groeperingen maken tijdens hun kleinschalige digitale aanvallen ook gebruik van misleiding. Het is voorgekomen dat jihadisten socialemedia-accounts van het Amerikaanse leger overgenomen hadden. Ze claimden gevoelige gegevens te hebben gestolen, afkomstig van dezelfde server.[105] Meerdere malen werden er persoonlijke gegevens van Amerikaans defensiepersoneel online vrijgegeven.[106][107]

In alle gevallen bleken deze 'gevoelige gegevens' echter openbaar verkrijgbare informatie te zijn, die jihadistische groeperingen waarschijnlijk in het bezit gekregen hebben door gerichte zoekopdrachten op internet.[108] Vooralsnog lijkt het hier dus niet te gaan om datalekken of nieuwe digitale capaciteiten van terroristen.

Deze vorm van misleiding heeft waarschijnlijk het voeren van propaganda als voornaamste motief. Omdat het vaak niet direct duidelijk is of er inderdaad gevoelige gegevens openbaar zijn gemaakt of niet, kunnen deze acties in potentie maatschappelijke onrust veroorzaken. Zij vormen echter geen direct gevaar voor de nationale veiligheid.

Cybervandalen en scriptkiddies

Activiteiten van cybervandalen en activisten krijgen veel media-aandacht, maar vormden in deze periode slechts een beperkte dreiging voor organisaties. Cybervandalen hebben een gevarieerd kennisniveau en voeren hacks uit omdat het kan of om aan te tonen dat zij er toe in staat zijn. Scriptkiddies zijn hackers met beperkte kennis die aanvallen uitvoeren vanuit baldadigheid en het zoeken naar een uitdaging.

94 https://www.aivd.nl/@3247/jaarverslag-aivd/
95 https://www.nctv.nl/onderwerpen/tb/dtn/
96 http://www.iss.europa.eu/uploads/media/Brief_2_cyber_jihad.pdf
97 http://securityaffairs.co/wordpress/36883/cyber-crime/cyber-caliphate-electronic-war.html
98 https://www.aivd.nl/@3247/jaarverslag-aivd/ en CSBN-4
99 https://citizenlab.org/2014/12/malware-attack-targeting-syrian-isis-critics/
100 https://www.youtube.com/channel/UCTDqtFI2EZG1Nrkr9zjZxbg
101 http://grugq.tumblr.com/post/109088631293/isis-compilation-of-intelligence-and-security
102 http://www.dailymail.co.uk/news/article-3029500/How-Snowden-helped-three-terror-groups-Al-Qaeda-linked-extremists-said-changed-way-communicate-leaks-traitor.html
103 http://blog.sensecy.com/2015/02/02/al-qaedas-electronic-jihad/
104 http://www.bbc.com/news/technology-28418951
105 http://www.washingtonpost.com/blogs/the-switch/wp/2015/01/12/the-centcom-hack-that-wasnt/
106 http://www.militarytimes.com/story/military/pentagon/2015/03/23/pentagon-notifying-troops-named-by-alleged-islamic-state-hackers/70332846/
107 http://www.washingtonpost.com/blogs/the-switch/wp/2015/01/12/the-centcom-hack-that-wasnt/
108 Zie noot 110 en http://www.militarytimes.com/story/military/pentagon/2015/03/23/pentagon-notifying-troops-named-by-alleged-islamic-state-hackers/70332846/.

Naast de beperkte dreiging die van deze groep uitgaat, kunnen aanslagen en incidenten voor deze groep een katalysator vormen voor eenvoudige digitale activiteiten, zoals DDoS-aanvallen en defacements. Zie ook het kader Digitale aanvallen en conflicten, aanslagen en incidenten.

Het afgelopen jaar vonden er in Nederland en in het buitenland digitale aanvallen plaats waarvan het vaak niet duidelijk was of zij door jihadisten waren gepleegd of door vandalen. Dit is vaak het geval bij DDoS-aanvallen of defacements waarbij een verwijzing naar ISIS wordt gemaakt, maar waarbij het niet zeker is of er ook een jihadistisch motief achter zit. De verwijzing naar ISIS gebruiken cybervandalen of scriptkiddies expres als misleiding of voor een shockerend effect en de media-aandacht die deze verwijzing teweeg brengt.[109]

Het afgelopen jaar zagen we cybervandalen en scriptkiddies verwijzen naar ISIS bij DDoS-aanvallen op onlinegaming-platformen[110] en de defacement van de website van Malaysian Airlines.[111]

Dit soort aanvallen kunnen in de toekomst maatschappelijk onrust veroorzaken als drukbezochte sites worden aangevallen, veelgebruikte diensten wegvallen of als webpagina's met maatschappelijke relevantie worden aangevallen.

Hacktivisten

Hacktivisten willen ideologische doelen realiseren of dichterbij brengen door digitale aanvallen. Onder deze groep actoren vallen ook hackers met ideologische motieven of patriottische hackers. Vaak kunnen aanvallen vanuit deze groep actoren in geopolitieke context geplaatst worden. Het afgelopen jaar vormden hacktivisten een relatief kleine dreiging voor Nederland.

Het gaat hier dan meestal om eenvoudige digitale activiteiten, zoals DDoS-aanvallen en defacements. Soms claimen deze groepen vertrouwelijke gegevens van de tegenstander gestolen te hebben.[112]

Het risico op digitale aanvallen van hacktivisten neemt toe tijdens intra- en internationale conflicten, aanslagen en incidenten. Zie ook het kader Digitale aanvallen en conflicten, aanslagen en incidenten. Ook kunnen de capaciteiten van deze groep toenemen nu hulpmiddelen om digitale aanvallen te plegen laagdrempeliger worden.

Interne actoren

Interne actoren zijn individuen die (tijdelijk) in een organisatie aanwezig zijn of zijn geweest, zoals (ex-)medewerkers, inhuurkrachten en leveranciers.

Het afgelopen jaar toonde aan dat financiële, politieke of persoonlijke motieven niet altijd de oorzaak zijn van het aantasten van de betrouwbaarheid van een (informatie)systeem. Ook onoplettendheid en menselijke fouten kunnen een rol spelen.

Bij diverse incidenten die dit jaar plaatsvonden, plaatsten medewerkers gevoelige informatie op privéservers en was deze informatie via het internet in te zien en te downloaden. Zo plaatste een medewerker van een verzekeraar declaratiegegevens van 27.000 verzekerden op een eigen server voor het testen van software.[113] Ook zette een systeembeheerder bij de politie gevoelige onderzoeksinformatie op een privésite. Deze informatie was vervolgens op het internet terug te vinden.[114]

Ook de beschikbaarheid van (informatie)systemen kan door menselijke fouten aangetast worden. Een fout bij onderhoudswerkzaamheden leidde bijvoorbeeld in mei 2015 tot een storing bij internetknooppunt AMS-IX.[115] Daardoor waren diverse websites en andere diensten tijdelijk niet of beperkt beschikbaar. Omdat de AMS-IX een van de grootste internetknooppunten van de wereld is, waren de gevolgen ook in het buitenland te merken. De storing was van korte duur: volgens AMS-IX heeft deze hoogstens tien minuten geduurd.[115]

Cyberonderzoekers

Cyberonderzoekers zoeken kwetsbaarheden in ICT-omgevingen om (te) zwakke beveiliging aan de kaak te stellen. Zij gebruiken vaak de media om hun bevindingen te publiceren en de bewustwording over cybersecurity te vergroten. Publiciteit over die kwetsbaarheden kan instellingen en bedrijven (tijdelijk) extra kwetsbaar maken, omdat kwaadwillenden dan kunnen profiteren van de onderzoeksbevindingen. In sommige gevallen verdenkt men de cyberonderzoeker zelf van strafbare feiten.

Het komt met enige regelmaat voor dat onderzoekers of journalisten kwetsbaarheden aan willen tonen en daardoor in aanraking met justitie komen. Dit gebeurde bijvoorbeeld toen Tweede Kamerleden vorig jaar doelwit waren geworden van een phishingaanval van een televisieprogramma, dat een beveiligingslek wilde aantonen.

109 http://www.theguardian.com/world/2015/jan/26/malaysia-airlines-website-hacked-by-lizard-squad
110 http://krebsonsecurity.com/2014/12/cowards-attack-sony-playstation-microsoft-xbox-networks/
111 http://www.thestar.com.my/News/Nation/2015/01/26/MAS-website-hacked-ISIS/
112 http://www.bbc.com/news/world-europe-30453069
113 http://www.cooperatievgz.nl/newsroom/verdere-aanscherping-procedures-vertrouwelijke-informatie
114 http://www.volkskrant.nl/binnenland/gevoelige-informatie-op-straat-door-veiligheidslek-politie~a3793726/
115 http://tweakers.net/nieuws/103067/internetknooppunt-ams-ix-kampt-met-uitval-update-2.html

De phishing-e-mail vroeg de ontvangers om op een phishingsite allerlei persoonlijke gegevens in te vullen. De aanval werd op tijd ontdekt en er werd aangifte gedaan bij de politie. Deze heeft de zaak nog in onderzoek.[116]

Sinds de publicatie van de Leidraad om te komen tot een praktijk van responsible disclosure[117] in 2013 kunnen cyberonderzoekers samen met de ICT-securitygemeenschap kwetsbaarheden op een vertrouwelijke en verantwoorde manier gemeld krijgen door middel van een van waarborgen voorziene handelswijze. De richtlijn heeft als doel om melders te faciliteren en tot een snelle oplossing van kwetsbaarheden te komen.[118]

Responsible disclosure wordt vaker en door meer organisaties toegepast. Hoofdstuk 5 bespreekt de stand van zaken van responsible disclosure in Nederland.

Private organisaties

Private organisaties kunnen de vertrouwelijkheid van informatie(systemen) aantasten voor financieel gewin. Ook kunnen zij zich schuldig maken aan bedrijfsspionage om hun concurrentiepositie te verbeteren. Het is niet de verwachting dat digitale bedrijfsspionage in dreigingsniveau veel zal verschillen van fysieke bedrijfsspionage. Op het gebied van digitale bedrijfsspionage zijn geen nieuwe trends of fenomenen waargenomen waarvan dreiging uitgaat.

Digitale aanvallen en conflicten, aanslagen en incidenten

Verschillende actoren grijpen intra- en internationale conflicten, aanslagen en incidenten vaak aan als aanleiding voor digitale aanvallen. Het afgelopen jaar zijn er bijvoorbeeld veel digitale aanvallen waargenomen die in geopolitieke context geplaatst kunnen worden, zoals de malware-aanvallen die zijn te relateren aan het conflict in Oekraïne. Het is vaak erg moeilijk om de aanvallen aan partijen toe te schrijven. Zowel statelijke actoren als activistische hackers met patriottische motieven hebben de intenties en de middelen om deze aanvallen uit te voeren.[119]

Ook aanslagen, rampen en incidenten kunnen situaties creëren waarbij partijen door digitale activiteiten informatie willen inwinnen. Deze situatie deed zich vorig jaar voor bij een gerichte digitale aanval op Maleisische overheidsfunctionarissen en medewerkers van Malaysian Airlines die de verdwijning van vlucht MH370 onderzochten. Het vermoeden is dat de aanvallers hierbij op zoek waren naar documentatie gerelateerd aan het onderzoek naar MH370 en deze gegevens vervolgens gestolen hebben.[120] Ook zou tijdens internationale contacten over vlucht MH17 de telefoon van de Australische minister van Buitenlandse Zaken gecompromitteerd zijn.[121]

Hoewel de herkomst en motieven van deze aanvallen altijd moeilijk met zekerheid vast te stellen zijn, is het voorstelbaar dat partijen belang kunnen hebben bij het onderscheppen van informatie en standpunten over deze gebeurtenissen.

Criminelen gebruiken aanslagen, rampen en incidenten vaak als middel om geld te verdienen. Zowel de Charlie Hebdo-aanslagen als de ramp met vlucht MH17 zijn door criminelen aangegrepen om door middel van klikfraude en advertenties inkomsten te genereren, of om malware te verspreiden.[122] Zij deden dit bijvoorbeeld door valse profielen van slachtoffers van de vliegramp aan te maken.[123] Ook probeerden criminelen systemen te compromitteren door het verspreiden van malware in foto's of videoplayers om filmpjes van de crash te bekijken.[124]

Aanslagen en incidenten vormen een katalysator voor aanvallen met ideologische motieven. Het gaat hier dan meestal om eenvoudige digitale activiteiten, zoals DDoS-aanvallen en defacements. In het begin van 2015 vormden de aanslag op de Charlie Hebdo-redactie in Parijs het startschot van diverse digitale aanvallen in Frankrijk. Meestal werden deze uitgevoerd door pro-jihadistische partijen die een ideologische daad wilden stellen.[125] Als reactie op deze aanvallen richtte hackerscollectief Anonymous zich op het deactiveren van socialemedia-accounts en websites van pro-jihadistische partijen.[126 127]

116 https://www.security.nl/posting/416784/Mogelijk+boete+voor+phishingaanval+op+Kamerleden
117 https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html
118 http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/12/19/tk-voortgang-responsible-disclosure.html
119 http://www.crowdstrike.com/2014-global-threat-report/
120 http://www.thestar.com.my/News/Nation/2014/08/20/Hacker-targets-info-on-MH370-probe-Computers-of-officials-infected-with-malware/
121 http://www.heraldsun.com.au/news/foreign-minister-julie-bishops-phone-was-hacked-at-the-height-of-the-mh17-crisis/story-fniofiyv-1227026241325
122 https://www.bluecoat.com/security-blog/2015-01-14/miscreants-say-je-suis-charlie-too
123 http://nos.nl/op3/artikel/677528-grof-geld-verdienen-met-mh17kliks.html
124 https://www.security.nl/posting/397457/Zogenaamde+raketvideo+MH17+verspreidt+ongewenste+software
125 http://www.newsweek.com/19000-french-websites-and-counting-hacked-charlie-hebdo-attack-299675
126 http://www.nu.nl/internet/3969091/anonymous-belooft-enorme-reactie-aanslag-in-parijs.html
127 http://www.independent.co.uk/life-style/gadgets-and-tech/opcharliehebdo-anonymous-take-down-french-extremist-website-after-threatening-retribution-for-charlie-hebdo-attacks-9972013.html

Tabel 2 **Actoren en hun intenties**

Actor	Intenties
Beroepscriminelen	Geldelijk gewin (direct of indirect)
Statelijke actoren	Geopolitieke (of interne) machtspositie verbeteren
Terroristen	Maatschappelijke verandering bewerkstelligen, bevolking ernstige vrees aanjagen of politieke besluitvorming beïnvloeden
Cybervandalen en scriptkiddies	Aantonen van kwetsbaarheden, hacken omdat het kan, baldadigheid, zoeken van uitdaging
Hacktivisten	Ideologische motieven
Interne actoren	Wraak, geldelijk gewin, ideologische motieven (mogelijk 'aangestuurd')
Cyberonderzoekers	Aantonen zwakheden, eigen profilering
Private organisaties	Verkrijging waardevolle informatie

Conclusie en vooruitblik

De grootste digitale dreiging is nog altijd afkomstig van criminelen en statelijke actoren.

Criminelen zijn goed georganiseerd en worden creatiever met het verzilveren van gestolen gegevens. Zij zijn ook bereid veel tijd te steken in het voorbereiden van aanvallen. De dreiging die uitgaat van zowel vernieuwende als traditionele aanvallen van criminelen zal verder toenemen.

Digitale aanvallen zijn voor statelijke actoren nog altijd een aantrekkelijk alternatief voor conventionele militaire en spionagemiddelen, vanwege de grote omvang en impact tegen lage kosten en afbreukrisico's. Hierdoor zal het aantal actoren dat een potentiële dreiging kan vormen voor de nationale veiligheid verder toenemen.

Door deze toename van het aantal actoren (zowel statelijk als crimineel) zal het in de toekomst bovendien moeilijker worden om digitale aanvallen aan partijen toe te schrijven.

Jihadistische groeperingen beginnen gebruik te maken van laagdrempelige malware, maar toch is het merendeel van de aanvallen nog kleinschalig en eenvoudig. Er zijn geen aanwijzingen voor een concrete dreiging richting Nederland. Bij defacements is het vaak niet duidelijk of zij door een jihadistische actor zijn gepleegd of door vandalen. Wel maakt de toenemende beschikbaarheid van geavanceerde malware op het internet het voorstelbaar dat de digitale capaciteiten van jihadistische groeperingen in de toekomst verder zullen toenemen.

Ten slotte vormen conflicten, aanslagen en incidenten voor verschillende actoren aanleiding om digitale aanvallen uit te voeren. Statelijke actoren, criminelen en actoren met ideologische motieven gebruiken deze situaties om hun doelstellingen te verwezenlijken.

Door het succes van spearphishing is deze vorm van social engineering de primaire aanvalsvector voor digitale spionage.



3 Dreigingen: Middelen

De middelen die actoren tot hun beschikking hebben, zijn geavanceerder geworden. Voor actoren met beperkte kennis zijn er meer kant-en-klaarmiddelen. Ransomware ontwikkelt zich verder, wordt professioneler en richt zich op meer verschillende systemen. Ook op andere gebieden blijven kwaadwillenden op zoek naar vernieuwing om ervoor te zorgen dat aanvallen succesvol en effectief blijven. Zo blijven aanvallers bij DDoS-aanvallen op zoek naar nieuwe amplificatie-methoden, proberen malwareschrijvers op diverse manieren detectie te omzeilen en zijn spearphishingaanvallen moeilijker te herkennen.

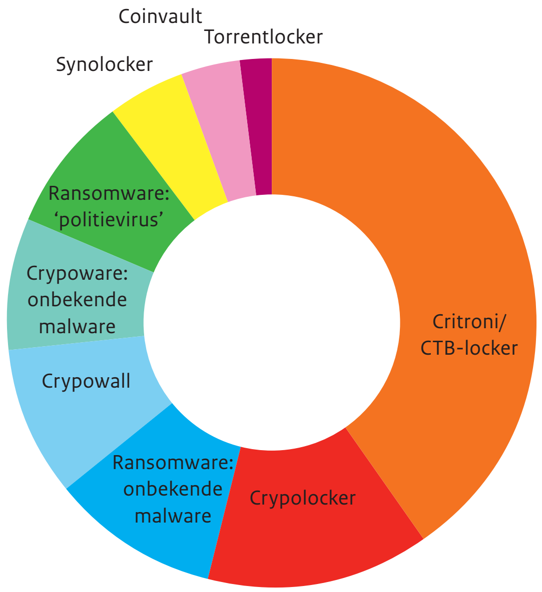
Actoren maken bij digitale aanvallen gebruik van middelen om kwetsbaarheden te misbruiken of te vergroten. Het kan zowel om technische middelen als om aanvalsmethoden gaan. Dit hoofdstuk gaat in op deze middelen.

Malware

Ransomware professionaliseert verder en vormt een groeiend probleem

De hoeveelheid ransomware (en cryptoware, zie tekstkader op de volgende pagina) groeit verder. Het Team High Tech Crime (THTC) van de politie ziet dat de opkomst van cryptoware in Nederland, die in het vorige CSBN al werd voorspeld, in de periode van dit CSBN werkelijkheid is geworden. Verschillende cryptoware-campagnes, zoals Critroni/CTB-Locker, Cryptolocker en Cryptowall, maakten in deze periode Nederlandse slachtoffers. Dat blijkt uit aangiftes bij de Nederlandse politie. Het overzicht uit figuur 1 is gebaseerd op 87 aangiftes die in de rapportageperiode binnenkwamen bij de politie en die op basis van zoektermen werden teruggevonden in de politiesystemen. Van de 75 aangevers waarvan bekend is of ze wel of niet hebben betaald, heeft circa 10 procent het losgeld betaald. Dit percentage is internationaal gezien vrij hoog. Dat het aantal aangiftes laag is ten opzichte van het aantal besmettingen wordt duidelijk door de casus Coinvault (kader in Hoofdstuk 1). Ongeveer 1,5 procent van de slachtoffers betaalde losgeld. Mogelijk zijn slachtoffers die betaald hebben gemotiveerder om aangifte te doen dan slachtoffers die niet betaald hebben.

Figuur 1 **Aangiftes ransomware in Nederland**[128]



128 Bron: politie.

Ransomware versus cryptoware

Ransomware is malware die de toegang tot een systeem onmogelijk maakt. Het slachtoffer moet een geldbedrag overmaken aan de crimineel om dit ongedaan te maken. Het zogenaamde 'politievirus'[129] van enige tijd geleden, waarbij de gebruiker de melding krijgt dat hij zich schuldig zou hebben gemaakt aan strafbare feiten, is hiervan een voorbeeld.

Cryptoware is een vorm van ransomware. Hierbij gaan criminelen nog een stap verder door ook bestanden op het systeem van de gebruiker te versleutelen. Ontsleuteling van deze bestanden kan alleen via een geheime sleutel, in het bezit van de criminelen. Het slachtoffer krijgt die alleen door te betalen. Overigens is dat geen garantie voor het verkrijgen van de sleutel en de originele bestanden. De politie adviseert daarom met klem om niet te betalen.[130]

Nieuwe varianten van dit type malware verschijnen frequent en de opbrengsten die criminelen realiseren zijn hoog. Zo wees een analyse van bitcoinbetalingen door Fox-IT uit dat de makers van de TorrentLocker-ransomware vermoedelijk ruim 250.000 euro verdienden met hun criminele praktijken, afkomstig van minimaal 653 slachtoffers. Vermoedelijk is de opbrengst van een betaling dus enkele honderden euro's per persoon.[131]

Vanwege de financiële beloning verbeteren criminelen continu hun malware en hun aanpak om zodoende het succes ervan – en de inkomsten die ermee gepaard gaan – verder te laten groeien. De ontwikkelaars van ransomware maakten in het verleden nog wel eens technische fouten. Daardoor was het bijvoorbeeld mogelijk om versleutelde bestanden terug te krijgen via een sleutel die achterbleef op het systeem[132] of via schaduwkopieën van Windows.[133] In nieuwere versies van ransomware kan dit niet meer en is het slachtoffer aangewezen op back-ups of veroordeeld tot het betalen van het bedrag aan de crimineel dat veelal varieert tussen de 100 en 700 euro.[134]

Via diverse hulpmiddelen proberen de criminelen achter ransomware de herleidbaarheid van individuen en de technische infrastructuur achter deze infrastructuur te verminderen. Zij maken meer gebruik van anonimiseringsnetwerken als Tor en I2P[135] voor netwerkcommunicatie en van bitcoin of andere cryptocurrency's voor het innen van het gevraagde bedrag. Zo maakt Critroni, ransomware die door cybercriminelen online te koop wordt aangeboden voor een bedrag van rond de 1500 dollar, gebruik van Tor voor communicatie met de servers van de crimineel. Als het slachtoffer geen Tor-software op zijn systeem heeft geïnstalleerd, maakt de malware automatisch verbinding met een online Tor-browser om de verbinding alsnog tot stand te kunnen brengen. Hierdoor kan de dader zichzelf goed afschermen voor opsporing.

Ransomware wordt breder ingezet

Criminelen willen nieuwe doelgroepen aanvallen met hun ransomware en daarmee meer effect sorteren. Dat blijkt uit het aanvallen van meer besturingssystemen (inclusief mobiele platformen) en het aanvallen van zakelijke gebruikers, naast de groep consumenten die al langer slachtoffer is.

Naast het versleutelen van bestanden op het systeem, vergrendelen aanvallers ook bestanden op bijvoorbeeld SD-kaarten, USB-sticks en netwerkbronnen, zelfs als deze netwerkbronnen niet gekoppeld zijn aan het systeem van de gebruiker.[136]

Een bijzondere vorm van cryptoware, Ransomweb, nestelt zich via een kwetsbaarheid op webservers. Daarna versleutelt het ongemerkt informatie in de database van deze website gedurende een langere tijd (bijvoorbeeld zes maanden) en ontsleutelt die weer op basis van een geheime sleutel. Voor opslag van deze sleutel gebruikt de crimineel een externe server die onder zijn controle staat.[137] Na een bepaalde periode verwijdert de aanvaller deze externe sleutel en is de informatie in de database niet meer toegankelijk. Dan pas komt de eigenaar erachter dat delen van de database – en de back-ups hiervan – niet meer leesbaar zijn. Uiteraard beloven de criminelen ook hier de eigenaar van de website om de sleutel te geven na betaling van het geëiste geldbedrag.

De manier waarop cybercriminelen hun slachtoffers besmetten met ransomware varieert. In veel gevallen reageren slachtoffers op e-mails uit naam van bekende bedrijven. In die e-mails verleiden ze de gebruiker om een geïnfecteerd bestand te openen of een malafide website te bezoeken. Daarnaast is bekend dat criminelen uit naam van Microsoft in sommige gevallen telefonisch contact opnemen en ransomware verspreiden via malafide bestanden in nieuwsgroepen.

129 https://www.politie.nl/themas/ransomware.html
130 https://www.politie.nl/nieuws/2014/maart/10/11-politie-waarschuwt-voor-cryptolock.html
131 http://blog.fox-it.com/2014/10/21/update-on-the-torrentlocker-ransomware/
132 http://www.itworld.com/article/2697593/security/mistake-in-ransomware-program-leaves-decryption-key-accessible.html
133 https://technet.microsoft.com/en-ie/magazine/2006.01.rapidrecovery%28en-us%29.aspx
134 Afhankelijk van de koers van de bitcoin.
135 http://blog.trendmicro.com/trendlabs-security-intelligence/android-ransomware-uses-tor/
136 http://www.bleepingcomputer.com/forums/t/569157/cryptofortress-a-torrentlocker-clone-that-also-encrypts-unmapped-network-shares/
137 https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html

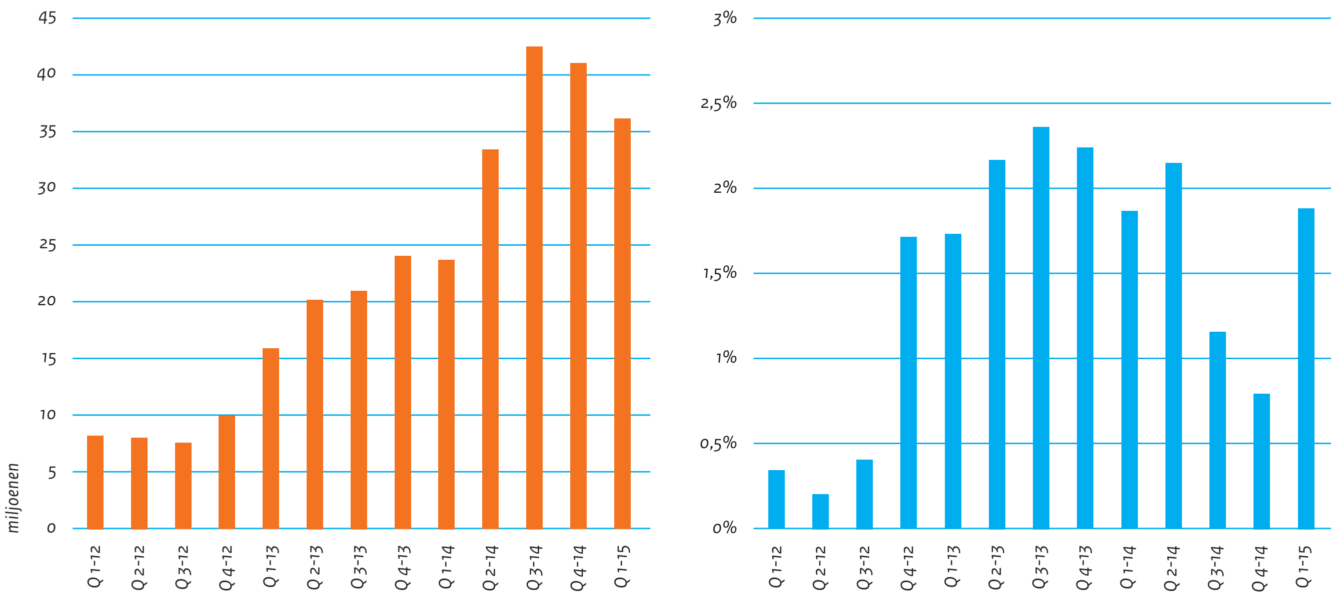
Het probleem van ransomware zal de komende periode vermoedelijk groeien, omdat het gijzelen van systemen of data tot nu toe succesvol is en op alle digitale systemen is toe te passen. De aanpak van cryptoware blijft een aandachtspunt. De geheime sleutel, die nodig is om bestanden en toegang te kunnen herstellen, is meestal alleen te verkrijgen door criminelen te betalen. In enkele gevallen achterhaalden private organisaties sleutels, waardoor slachtoffers zonder betaling hun bestanden konden ontsleutelen. Zo gaven Fox-IT en Kaspersky Lab geheime sleutels terug aan slachtoffers. Fox-IT deed dit door het kraken van het algoritme van de sleutels van Cryptolocker[138] en Kaspersky Lab door het ontsluiten van sleutels die werden aangetroffen op de server van een crimineel.[139] Preventie door middel van back-ups blijft echter de belangrijkste maatregel om de potentiële schade door ransomware te beperken.

Het risico op malware op mobiele platformen is nog altijd beperkt

Hoewel malware voor mobiele platformen wel bestaat, is de dreiging die hiervan uitgaat vooralsnog beperkt. Misbruik is meestal gericht op Android (94 tot 98 procent)[140 141] en in mindere mate op iOS (maximaal 6 procent).[142] De volgende kanttekeningen zijn hierbij van belang:

- Van alle nieuw verkochte smartphones in 2014 was 81,5 procent een Android-toestel.[144] Het ligt daarom voor de hand dat mobielemalwareschrijvers zich vooral op dit mobiele platform richten.
- De meeste malware komt via malafide apps terecht op de apparaten van gebruikers. Android-gebruikers die alleen zijn aangesloten op de officiële Google Play Store maken een zeer kleine kans om een geïnfecteerde app te downloaden. Slechts één op de duizend apps zou malafide intenties hebben.[145] Bij de appstores van andere aanbieders ligt dit percentage vaak aanzienlijk hoger. Volgens cijfers van Google zelf heeft minder dan 1 procent van de Android-gebruikers een potentieel schadelijke app op zijn systeem bij gebruik van meerdere stores. Dit is 0,15 procent voor gebruikers die alleen zijn aangesloten op de Google Play Store.[146]
- De locatie van gebruikers – en de app stores waarvan zij gebruikmaken – lijkt een belangrijke factor te zijn. Zo zouden Androidgebruikers in China een veel hogere kans hebben om een malafide app te downloaden dan gebruikers in andere landen. In China wordt namelijk intensief gebruikgemaakt van

Figuur 2 **Aantal unieke malware-samples en aandeel Android-malware per kwartaal**[143]



138 https://www.decryptcryptolocker.com/
139 https://noransom.kaspersky.com/
140 http://www.symantec.com/security_response/publications/threatreport.jsp
141 http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf
142 https://know.elq.symantec.com/LP=1543
143 Bron: AV-Test Institute.
144 http://www.idc.com/getdoc.jsp?containerId=prUS25450615
145 https://www.pulsesecure.net/lp/mobile-threat-report-2014/
146 https://source.android.com/devices/tech/security/reports/Google_Android_Security_2014_Report_Final.pdf

stores van derde partijen in plaats van de officiële Google Play Store.[147 148] Deze stores bevatten vaak opnieuw verpakte apps uit de officiële store. Soms voegen criminelen daar malafide code aan toe. In sommige gevallen trachten criminelen deze nieuw verpakte apps ook in de officiële stores te plaatsen.[149]

Uit cijfers van AV-Test blijkt dat het totaal aantal unieke malware-samples over alle besturingssystemen ten opzichte van CSBN-4 is toegenomen, ook al laten het laatste kwartaal van 2014 en het eerste kwartaal van 2015 een lichte daling zien (figuur 2, links). Het aandeel van Androidmalware op deze nieuwe malware is ongeveer 2 procent (figuur 2, rechts). Dit percentage is al sinds het vierde kwartaal van 2012 redelijk constant en nam in de tweede helft van 2014 zelfs nog af.

De meeste mobiele malware richt zich op Android. Dat betekent niet dat gebruikers van andere mobiele platformen, zoals Apple iOS, gevrijwaard zijn van malware. In veel gevallen vereist een succesvolle aanval op iOS echter wel dat de gebruiker zijn device heeft gekraakt (jailbroken) zodat deze ook niet-erkende, en dus niet-vertrouwde, apps toestaat. Bekende voorbeelden van iOS-malware die het afgelopen jaar op dit gebied werden aangetroffen waren de Xsser mRAT[150], een RAT die voorheen alleen op Android-systemen werd aangetroffen, en Xagent[151], ingezet om informatie van gebruikers te vergaren. Eind 2014 werd echter ook de eerste malware voor iOS aangetroffen (WireLurker).[152] Voor WireLurker is het niet nodig dat een systeem is gekraakt. Deze malware scant en infecteert mobiele Apple-apparaten zodra ze op de USB-poort van een geïnfecteerd Apple Mac OS X-systeem worden aangesloten.

Ransomware en mobiele platformen

Ransomware richt zich niet meer alleen op Windows. Het is inmiddels ook gezien op mobiele platformen. Hoewel simpele blokkering van op Android gebaseerde apparaten al eerder plaatsvond, en nog altijd plaatsvindt (bijvoorbeeld ScarePackage[153]), dook vorig jaar de eerste cryptoware (Simplocker[154]) op. Net als bij de traditionele Windows-cryptoware versleutelt deze cryptoware bestanden op het systeem. Ook gebruikers van Apple iOS kregen te maken met een vorm van ransomware, alleen werden bestanden niet versleuteld. In deze zogenoemde Oleg Pliss-aanval toonden de aanvallers een melding op iOS-devices dat het apparaat geblokkeerd was. De aanvallers eisten wederom een geldbedrag om de blokkade op te heffen. Ze maakten waarschijnlijk misbruik van de Apple ID's van slachtoffers, maar het is vooralsnog onduidelijk hoe zij aan de inloginformatie hiervoor kwamen.[155]

Tools

Kant-en-klare tools vormen een populair hulpmiddel

In de vele publieke rapporten over geavanceerde aanvallen valt op dat aanvallers dankbaar gebruikmaken van tools die niet per definitie voor malafide doeleinden zijn ontwikkeld, maar soms ook voor het onderzoeken van systemen of het uitvoeren van penetratietesten. Aanvallers lijken het wiel niet opnieuw te willen uitvinden en kiezen daarom voor deze standaardtools. Denk hierbij aan SaaS-achtige diensten, zoals booterservices, die het uitvoeren van DDoS-aanvallen mogelijk maken via een website.

Een ander voorbeeld is MimiKatz, een tool die vooral geschikt is voor het achterhalen van wachtwoorden, Kerberos-tickets en hashes uit het geheugen van een Windows-systeem. Actoren gelieerd aan de Cleaver-[156], Hurricane Panda-[157] en Anunak-[158]/ Carbanak[159]-aanvallen achterhalen met deze tool inloggegevens van het Windows-netwerk en krijgen op die manier snel toegang tot vrijwel alle systemen binnen het netwerk.

In sommige gevallen gebruiken de aanvallers kant-en-klare exploits van het populaire Metasploit-raamwerk.[160] Met Metasploit kunnen aanvallers misbruik maken van bekende kwetsbaarheden en deze op verschillende manieren uitbuiten. Daarvoor hebben zij geen diepgaande kennis over de kwetsbaarheid of verder misbruik nodig. Hoewel de tool bedoeld is als hulpmiddel voor penetratie-testers, kunnen ook kwaadwillenden de tool inzetten om een digitale aanval uit te voeren.

147 https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2013.pdf
148 Een belangrijke reden voor het gebruik van deze alternatieve stores is dat in China alleen gratis apps uit de officiële Google Play Store geïnstalleerd kunnen worden; zie https://support.google.com/googleplay/answer/143779.
149 http://www.trendmicro.nl/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fake-apps.pdf
150 http://media.scmagazine.com/documents/98/xsser_mrat_-_akamai_advisory_24310.pdf
151 http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/
152 https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf
153 https://www.lookout.com/resources/reports/mobile-threat-report
154 http://www.welivesecurity.com/2014/06/04/simplocker/
155 http://www.zdnet.com/article/icloud-not-compromised-in-apple-id-attack-apple/
156 http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf
157 http://go.crowdstrike.com/rs/crowdstrike/images/GlobalThreatIntelReport.pdf
158 https://www.fox-it.com/en/files/2014/12/Anunak_APT-against-financial-institutions2.pdf
159 https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
160 Zie bijvoorbeeld https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf

Ook kant-en-klare exploits, exploitkits en malware zijn populair

Niet alleen tools, maar ook exploits, exploitkits en malware behoren tot het gereedschap van aanvallers. Het valt op dat diverse (typen) actoren gebruikmaken van dezelfde malware en dezelfde exploitkits, zoals de PlugX-RAT en de Angler-exploitkit.[161]

Publiek gemaakte exploits zijn vooral gericht op Windows- en PHP-applicaties

Het aantal publiek gemaakte exploits nam, net als in vorige periodes, ook in deze periode weer verder af (zie figuur 3, links). Een mogelijke verklaring is dat het moeilijker is geworden om exploits voor moderne software te schrijven.

Verdedigingsmechanismen als sandboxing en address space layout randomization (ASLR) worden in steeds meer producten gebruikt. Daarnaast blijken oudere exploits nog altijd bruikbaar voor aanvallers, omdat lang niet alle software up-to-date is. Een analyse van 276 openbare rapporten over APT's laat zien dat de meeste misbruikte kwetsbaarheden in gerichte aanvallen al enkele jaren oud zijn.[162]

Onderverdeeld naar platform richten de meeste exploits zich nog altijd op PHP-applicaties en applicaties op Windows-platformen. Een groot gedeelte van de exploits voor PHP-applicaties richt zich op (plug-ins voor) de populaire PHP-gebaseerde contentmanagementsystemen WordPress en Joomla (zie figuur 3, rechts). Dit aandeel nam in de afgelopen jaren iets verder toe. In de rapportageperiode vormen WordPress- en Joomla-exploits gezamenlijk iets meer dan 26 procent van het totaal aantal op PHP gerichte exploits. Een mogelijke verklaring voor het grote aandeel van deze exploits is dat WordPress en Joomla de meestgebruikte twee (opensource) contentmanagementsystemen zijn.[163]

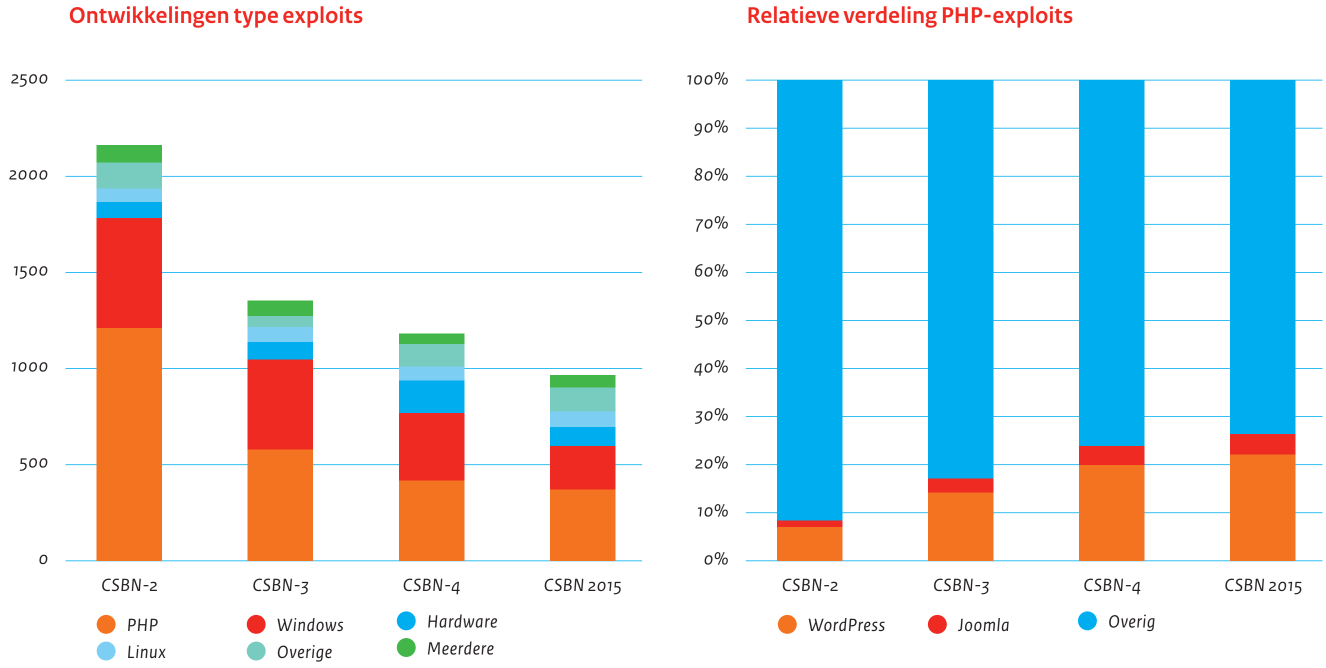
Exploitkits zijn vaker gericht op Adobe Flash

Diverse actoren maken gebruik van exploitkits om kwetsbaarheden uit te buiten. De exploits die in deze exploitkits zijn opgenomen geven een beeld van de software die zij misbruiken. Figuur 4 toont de ontwikkeling van ingebouwde exploits voor producten op basis van de inhoud van zestig verschillende exploitkits. Ten opzichte van het vorige CSBN is vooral Adobe Flash een populairder doelwit, terwijl de populariteit van Adobes pdf-producten is afgenomen.

RAT's worden misbruikt voor digitale betaalfraude in het mkb

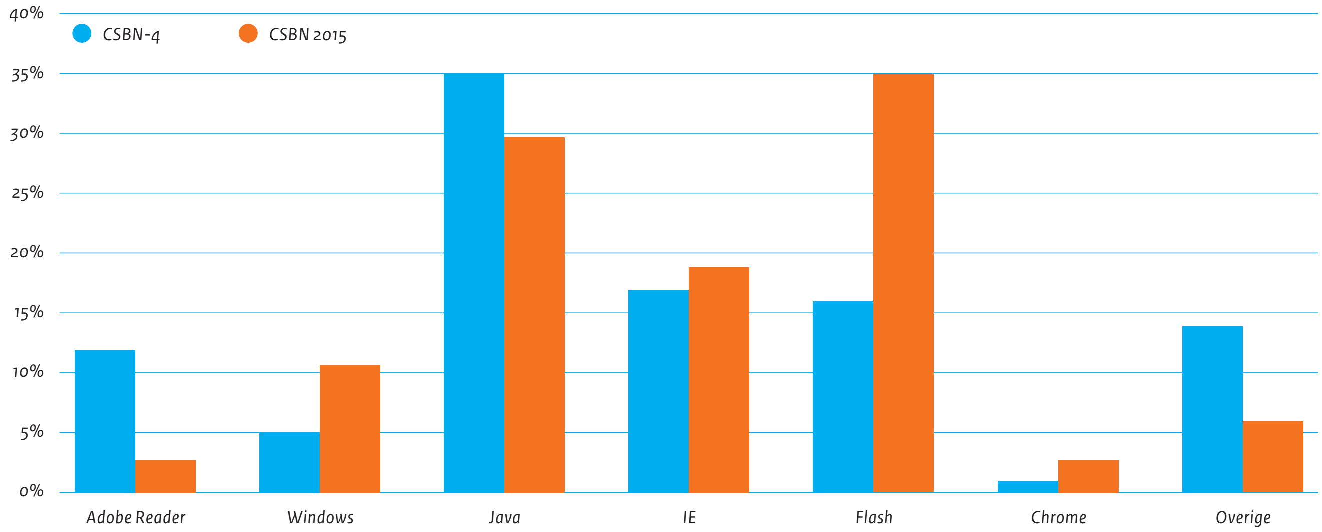
De politie constateert dat RAT's in Nederland vaker worden ingezet voor een nieuwe vorm van digitale betaalfraude. RAT's zijn relatief gemakkelijk te verkrijgen en te gebruiken. Het plegen van

Figuur 3 **Aantal gepubliceerde exploits per platform**[164 165]



161 http://www.crowdstrike.com/2014-global-threat-report/
162 Analyse op basis van APTnotes, een openbare lijst van APT-rapporten: https://github.com/kbandla/APTnotes (geraadpleegd op 13 juli 2015).
163 http://www.opensourcecms.com/general/cms-marketshare.php
164 Bron: http://exploit-db.com/.
165 Toelichting bij de labels in de linkerfiguur: exploits in de categorie 'Overige' richten zich op een ander platform (bijvoorbeeld Android of ARM) terwijl exploits in de categorie 'Meerdere' zich richten op meerdere platformen tegelijk (bijvoorbeeld Windows en Linux).

Figuur 4 **Producten als doelwit in exploitkits**[166]



bijvoorbeeld digitale fraude wordt daardoor laagdrempelig en toegankelijk voor verschillende dadergroepen.
De inzet van een RAT voor betalingsfraude is nieuw en lijkt zich vooralsnog op het mkb te richten. Besmetting komt door zakelijke (spear)phishing-e-mails. De criminelen gebruiken de RAT om toegang te krijgen tot verschillende betaalomgevingen van het bedrijf, bijvoorbeeld de internetbankieromgeving of de financiële administratie. Vervolgens proberen zij geld weg te sluizen naar geldezels en volgt een witwasproces.

Het is op dit moment nog niet bekend hoe groot de omvang en de schade van deze nieuwe vorm van digitale fraude is. De implicaties kunnen echter aanzienlijk zijn:
- De impact van deze fraudevorm kan groot zijn in de zin van economische en reputatieschade. Bovendien is de integriteit van het zakelijke betalingsverkeer in het geding.
- Het gaat om een relatief laagdrempelige vorm van cybercrime, die door een brede groep fraudeurs gepleegd kan worden. De gebruikte malware is goedkoop, makkelijk te krijgen en met beperkte digitale kennis te gebruiken.

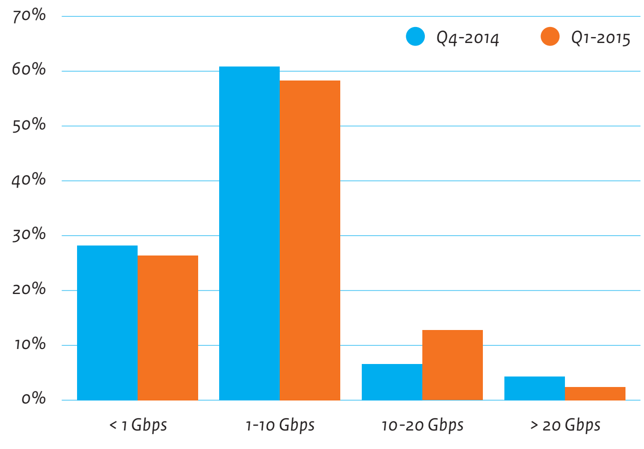
Denial-of-Serviceaanvallen

DDoS-aanvallen houden aan, maar zorgen voor beperkte verstoringen

DDoS-aanvallen vinden nog altijd plaats, maar zorgen in Nederland in beperkte mate voor verstoringen. De anti-DDoS-maatregelen die veel organisaties in Nederland troffen, lijken succesvol te zijn. Hoewel deze maatregelen de impact van DDoS-aanvallen beperken, vereist het wel een continue investering in veelal kostbare oplossingen. Alleen de symptomen worden bestreden, de aanvallen zelf blijven plaatsvinden.

Rapporten[167] over DDoS-aanvallen schetsen het beeld dat het maximale volume van aanvallen verder toeneemt tot circa 400 Gbps. De gemiddelde bandbreedte van een DDoS-aanval lijkt, alhoewel nog altijd fors, een stuk lager te zijn met volumes tussen de 8 en 12 Gbps. Deze volumes komen meer overeen met de

Figuur 5 **Volume van DDoS-aanvallen**[168]



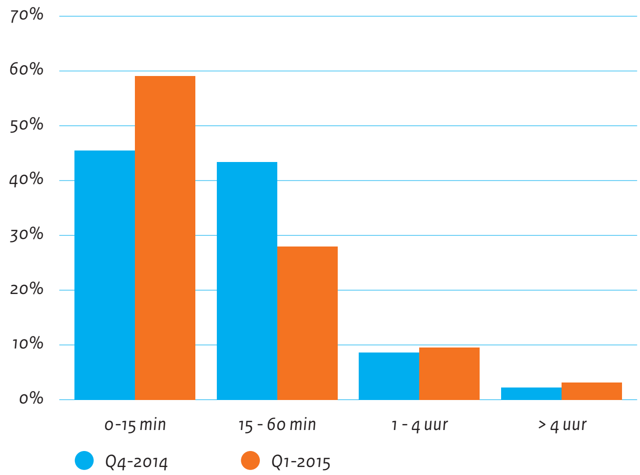
166 Bron: http://contagiodump.blogspot.com/, geraadpleegd mei 2015: https://docs.google.com/spreadsheet/ccc?key=0AjvsQV3iSLa1dE9EVGhjeUhvQTNReko3c2xhTmphLUE&usp=drive_web#gid=0.

167 DDoS-rapporten van Akamai, Arbor Networks, Black Lotus, BT, Corero, Link11, Kaspersky, Neustar, NSFOCUS, Radware, Symantec en Verisign zijn hiervoor bekeken.

168 Bron: georganiseerde Nederlandse groep aanbieders.

aanvallen die de doelgroepen van het NCSC zien en die ervaren worden door een Nederlandse groep van aanbieders die gezamenlijk een anti-DDoS-oplossing heeft geïmplementeerd. Uit cijfers van deze laatste groep blijkt dat bijna 85 procent van de aanvallen in het eerste kwartaal van 2015 minder dan 10 Gbps aan volume hadden (zie figuur 5). Dit laatste is wel iets minder in vergelijking met het laatste kwartaal van 2014. Toen kwam nog bijna 90 procent van de aanvallen niet boven de 10 Gbps uit.
Een andere belangrijke constatering is dat de duur van een

Figuur 6 **Duur van DDoS-aanvallen**[168]



gemiddelde DDoS-aanval afneemt. Het grootste gedeelte van de aanvallen houdt binnen een half uur tot een uur weer op. Dat blijkt ook uit de cijfers van de eerder genoemde georganiseerde groep van Nederlandse aanbieders. 59 procent van de aanvallen eindigt al binnen 15 minuten en ruim 87 procent stopt binnen een uur (zie figuur 6). Soms duren aanvallen slechts 5 minuten. Dat kan duiden op het gratis testen van een booterservice waarmee het eenvoudig is een DDoS-aanval uit te voeren (zie het kader Gebruik van booterservices). In sommige gevallen constateert men dat de aanvallen weliswaar korter zijn, maar wel intensiever.

Aanvallers blijven op zoek naar nieuwe vormen van amplificatie

Om een DDoS-aanval zo effectief mogelijk te laten zijn, blijven aanvallers op zoek naar nieuwe manieren om de hoeveelheid data die zij genereren te vergroten. Amplificatie is de methode die aanvallers hiervoor inzetten: verstuur een klein verzoek en verwacht een groot antwoord. In extreme gevallen kan het

Gebruik van booterservices

De politie ziet dat actoren voor het uitvoeren van DDoS-aanvallen vaak gebruikmaken van zogenoemde booter- of stresserservices. Een dergelijke service maakt het mogelijk om een DDoS-aanval uit te voeren zonder inhoudelijke kennis (DDoS-as-a-service). Een booterservice combineert verschillende van de bekende DDoS-aanvalsvectoren. Gebruikers kunnen de services vaak voor een paar minuten gratis uitproberen, daarna moeten ze een klein bedrag betalen, bijvoorbeeld 2 dollar per uur.[169] Ze kunnen de service dan inzetten voor het uitvoeren van DDoS-aanvallen op willekeurige doelen.

antwoord bijna 360 keer zo groot zijn als de vraag waardoor de amplificatie enorm is.[170] Doordat amplificatieaanvallen gebruikmaken van UDP kan de aanvrager een willekeurig IP-adres opgeven waar de server het antwoord naar moet terugsturen. Uiteraard kiest de aanvaller hierbij voor het IP-adres dat hij wil overladen met verkeer. Door beperkte filtering van sommige netwerkbeheerders kunnen aanvallers een willekeurig IP-adres opgeven ('spoofen').

Voorheen was voornamelijk het protocol NTP een populair hulpmiddel voor het uitvoeren van DDoS-aanvallen. Door het uitkomen van een patch en het wijzigen van configuraties door NTP-beheerders, werd deze vorm van amplificatie minder succesvol en zochten aanvallers naar nieuwe vormen van amplificatie en andere DDoS-technieken. De afgelopen periode werden daardoor meer aanvallen zichtbaar die misbruik maken van andere UDP-gebaseerde protocollen zoals SSDP/UpnP[171], SNMP[172] en multicast DNS[173]. Onderzoekers toonden ook aan dat TCP-gebaseerde protocollen, naast de traditionele UDP-gebaseerde protocollen, een hoge mate van amplificatie kunnen veroorzaken.[174]

Obfuscatie

Het is voor actoren belangrijk om tijdens het uitvoeren van digitale aanvallen niet op te vallen, zo min mogelijk sporen achter te laten en moeilijk traceerbaar te zijn. Daarmee bemoeilijken zij ook de attributie van hun daden. Alle activiteiten die zij daarvoor ondernemen, worden obfuscatie genoemd.

Misbruik van bonafide diensten voor (versleutelde) communicatie

Het opsporen van verdacht verkeer binnen een netwerk is moeilijker door bonafide domeinnamen, websites en diensten voor

169 https://www.verisigninc.com/assets/report-ddos-trends-Q42014.pdf
170 https://www.us-cert.gov/ncas/alerts/TA14-017A
171 https://isc.sans.edu/forums/diary/1900UDP+SSDP+Scanning+and+DDOS/18599
172 http://www.prolexic.com/kcresources/white-paper/white-paper-snmp-ntp-chargen-reflection-attacks-drdos/An_Analysis_of_DrDoS_SNMP-NTP-CHARGEN_Reflection_Attacks_White_Paper_A4_042913.pdf
173 https://github.com/chadillac/mdns_recon
174 https://www.usenix.org/system/files/conference/woot14/woot14-kuhrer.pdf

Tabel 3 **Overzicht misbruik van bonafide diensten als communicatiekanaal**

Doel	Misbruikte dienst	Bijzonderheden
Configureren en aansturen van geïnfecteerde systemen	Dropbox[175 176]	Aanpassen C&C-instellingen bij gerichte aanvallen en het hosten van onderdelen van een exploit.
	Pinterest[177]	Voor het doorsturen van gebruikers naar malafide websites werd informatie over deze sites gecodeerd opgenomen in 'pins'.
	Reddit[178]	Lijst met C&C-servers opgenomen in een commentaar in een Reddit-post.
	Vkontakte[179]	Informatie over de C&C-server opgeslagen als een bericht op de "wall" van gebruikers van dit sociale netwerk.
	Google Docs[180]	Informatie over de C&C-server via steganografie verwerkt in een bmp-bestand op Google Docs.
	Microsoft Technet[181]	IP-adressen van C&C-servers verwerkt in commentaren op een Technet Forum thread.
Exfiltreren data	Gmail[182]	De aanvallers slaan data op in conceptberichten in Gmail.
	Video services[183]	Uploaden van videobestanden naar bijvoorbeeld YouTube met daarin steganografisch verborgen data.

communicatie door malware. Bij detectie wordt gebruikgemaakt van IP-adressen en domeinnamen waarvan bekend is dat zij betrokken zijn bij digitale aanvallen (malafide IP-adressen en domeinnamen). Daarom levert het gebruik van juist bonafide IP-adressen en domeinen geen waarschuwing op. Wanneer bonafide websites – of andere diensten – daarnaast ondersteuning bieden voor TLS-versleuteling, is bovendien ook niet inzichtelijk wélke informatie een systeem binnen het netwerk uitwisselt met een dergelijke website. Dit komt doordat detectiemiddelen op netwerkniveau geen inzicht hebben in het verkeer. Er kan dus alleen detectie zijn op de plekken waar de informatie weer wordt ontsleuteld (bijvoorbeeld op de werkplek van de gebruiker). Hoewel dit geen nieuwe ontwikkeling is, blijkt deze aanpak nog altijd in gebruik door aanvallers.

Tabel 3 toont een aantal recente voorbeelden van misbruik van bonafide diensten voor communicatie door malware. In de tabel is onderscheid gemaakt tussen gebruik van diensten voor het configureren en aansturen van geïnfecteerde systemen (informatie naar het geïnfecteerde systeem) en het exfiltreren van data (informatie vanuit het geïnfecteerde systeem). Het valt op dat de aanvallers, naast bonafide diensten, in sommige gevallen ook gebruik maken van steganografie om de communicatie te verhullen.

Malwareschrijvers omzeilen detectie door juist geen obfuscatie te gebruiken

Waarschijnlijk vertroebelen malwareschrijvers hun malware zoveel mogelijk om analyse door specialisten moeilijker te maken. Soms lijken aanvallers ervoor te kiezen dit juist niet te doen, zoals bij de foxy-[184] en Babar-malware. Dit maakt het ontleden van de malware door onderzoekers eenvoudiger, omdat bijvoorbeeld de code eenvoudiger te ontrafelen is. Het ontdekken van de malware binnen een netwerk is echter moeilijker. Het gebruik van obfuscatie- en versleutelingstechnieken door een programma is voor virusscanners en andere detectietools binnen een netwerk namelijk aanleiding om een programma te wantrouwen. Daarom gebruiken aanvallers dit bij gerichte aanvallen meestal niet.[185] Het voorkomen van herkenning is blijkbaar belangrijker dan het voorkomen van herkenning van de intenties en werkwijze van de malware.

Aanvalsvectoren

Aanvalsvectoren zijn methoden die aanvallers kunnen gebruiken om hun slachtoffer(s) aan te vallen. Een aanvalsvector is het vehikel waarmee de aanvaller probeert controle te krijgen over het systeem van de gebruiker. Deze paragraaf bespreekt een aantal afzonderlijke aanvalsvectoren die zich de afgelopen periode hebben

175 http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/
176 http://blogs.cisco.com/security/a-string-of-paerls/3
177 http://www.pcrisk.com/internet-threat-news/8568-trojan-leverages-pinterest-to-communicate-with-c-and-c-servers
178 http://news.drweb.com/show/?i=5977&c=5&lng=en&p=0
179 http://community.websense.com/blogs/securitylabs/archive/2015/01/30/new-foxy-malware-employs-cunning-stealth-amp-trickery.aspx
180 http://blog.airbuscybersecurity.com/post/2014/12/Vinself
181 https://www2.fireeye.com/WEB-2015RPTAPT17.html
182 http://www.wired.com/2014/10/hackers-using-gmail-drafts-update-malware-steal-data/
183 http://www.tripwire.com/state-of-security/incident-detection/hackers-exfiltrating-data-with-video-steganography-via-cloud-video-services/
184 http://community.websense.com/blogs/securitylabs/archive/2015/01/29/new-foxy-malware-employs-cunning-stealth-amp-trickery.aspx
185 Zie het rapport over de Babar-malware, https://drive.google.com/file/d/0B9Mrr-en8FX4dzJqLWhDblhseTA/view?pli=1.

voorgedaan. Aanvallers beperken zich meestal niet tot één specifieke aanvalsvector, maar combineren verschillende vectoren om hun doel te bereiken.

Phishing, in het bijzonder spearphishing, is hét middel voor gerichte aanvallen

In de afgelopen periode voerden criminelen alleen al in Nederland tientallen verschillende phishingcampagnes uit. De e-mails leken in veel gevallen afkomstig van betrouwbare partijen, zoals bol.com, post.nl[186], KPN, Intrum Justitia en alle grote banken.[187] Ook overheidsorganisaties zoals DigiD, de Belastingdienst en het Centraal Justitieel Incassobureau werden als afzender misbruikt. De nadruk ligt bij het bedrijfsleven, zo suggereren de incidentmeldingen bij het NCSC. 37 procent van de door private organisaties gemelde incidenten had te maken met phishing, tegen 16 procent voor overheden.[188]

Aanvallers waren vooral succesvol als ze gebruikmaakten van spearphishing. Eén persoon of een beperkte groep personen ontvangt dan een phishing-e-mail. Via deze e-mail proberen aanvallers bijvoorbeeld inloggegevens voor webmail van een medewerker te bemachtigen. Daarmee kunnen zij vervolgens verdere aanvallen uitvoeren op andere personen binnen de organisatie. In andere gevallen maken de aanvallers gebruik van geïnfecteerde bijlagen of links die verwijzen naar exploitkits om het systeem van hun slachtoffer te infecteren. Hoewel de aanvallers via deze bijlagen en links niet direct hengelen naar gevoelige informatie, valt ook dit type aanval onder de noemer spearphishing. Door het succes van spearphishing is deze vorm van social engineering de primaire aanvalsvector voor digitale spionage.

Naast spearphishing vormt ook klassieke phishing nog altijd een hulpmiddel van actoren. Aanvallers gebruiken spearphishing meestal om de systemen van hun slachtoffers te infecteren voor gevoelige informatie. Klassieke phishing heeft veel meer als doel om financieel gewin te behalen zonder daarbij een selecte groep aan slachtoffers uit te kiezen. Opvallend is dat Nederland een populair doelwit is voor phishers. Uit onderzoek van RSA blijkt dat in totaal 3 procent[189] tot 6 procent[190] van de wereldwijde phishing-e-mails zich richt op Nederlandse gebruikers. De populariteit van Nederland zou liggen in de relatief goede economische situatie en de sterke euro.[191] De schade als gevolg van phishing, gericht op Nederlandse banken, is echter wel afgenomen tot 3,9 miljoen euro in 2014 tegen 4,7 miljoen euro een jaar eerder.[192]

Wateringhole-aanvallen vormen een populaire aanvulling op spearphishing

Als een spearphish niet succesvol is, kiezen aanvallers regelmatig voor een tweede populair hulpmiddel bij gerichte aanvallen: een wateringhole. Bij een wateringhole-aanval verspreidt de aanvaller zijn exploits en malware via een website die veel van zijn slachtoffers regelmatig bezoeken door misbruik te maken van een kwetsbaarheid in deze website of een cms waarop de website gebaseerd is.[193] Daarna probeert de aanvaller meestal de systemen van bezoekers te infecteren via een exploit richting deze systemen. Het gebruik van deze drive-by-exploits via een dergelijke website is niet nieuw, maar vormt nog wel een reële dreiging. Een bijzondere aanvalsvector uit het afgelopen jaar was het plaatsen van geïnfecteerde software op een website van een leverancier van industriële routers. Klanten besmetten dan automatisch hun systemen met de Havex RAT bij het installeren van deze software.[194]

Malafide advertenties blijven een gevaar vormen voor internetgebruikers

Het gebruik van malafide advertenties door cybercriminelen (malvertising) vormt nog altijd een gevaar voor veel internetgebruikers. Advertenties zijn verwerkt in heel veel websites, waarvan sommige een groot aantal bezoekers trekken. Aanvallen met malafide advertenties zijn daarom een vorm van wateringhole-aanvallen. Eén malafide advertentie kan in korte tijd een hoge impact hebben, zeker als deze advertentie getoond wordt via websites als YouTube[195] of nu.nl.[196] Het openen van een website met daarop een malafide advertentie leidt er vaak toe dat geheel automatisch allerlei kwetsbaarheden op het systeem van de gebruiker worden uitgebuit. Vaak gebruiken malafide advertenties exploitkits, met daarin hoogwaardige exploits, waardoor de kans op succes voor de crimineel hoog is.
Cybercriminelen misbruiken advertentienetwerken tegenwoordig ook om een specifieke groep van gebruikers aan te vallen. Hiervoor maken zij gebruik van real-time-bidding (RTB)-advertentienetwerken. Advertenties worden dan op dynamische basis gekozen, onder andere afhankelijk van de eigenschappen van de gebruiker die de website bezoekt. Een RTB-netwerk biedt bonafide adverteerders de mogelijkheid om hun advertentie alleen aan te

186 https://www.security.nl/posting/405715/PostNL+waarschuwt+klanten+voor+besmette+e-mails
187 https://www.fraudehelpdesk.nl/sub-vragen/phishingmails/
188 Zie Bijlage 1: NCSC-statistieken.
189 http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-0614.pdf
190 http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-102014.pdf
191 http://www.nu.nl/internet/3389377/nederlanders-populair-doelwit-van-phishing.html
192 http://www.betaalvereniging.nl/wp-uploads/2015/03/150318-Fraude-betalingsverkeer-gehalveerd-20141.pdf
193 Zie bijvoorbeeld de werkwijze van de Waterbug-groep: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf.
194 https://www.f-secure.com/weblog/archives/00002718.html
195 http://blogs.cisco.com/security/talos/kyle-and-stan
196 http://tweakers.net/nieuws/97041/nu-punt-nl-verspreidde-malware-via-geinfecteerd-advertentienetwerk-update-2.html

bieden aan gebruikers die voldoen aan een bepaald profiel (bijvoorbeeld alleen personen met specifieke interesses afkomstig uit een specifiek land).

Het gebruik van een RTB-netwerk maakt dat malvertising niet alleen ongerichte drive-by-aanvallen mogelijk maakt, maar ook gerichtere aanvallen zoals bij wateringholes. Invincea zag bijvoorbeeld dat specifieke Amerikaanse defensiebedrijven werden aangevallen via malafide advertenties.[197] Dit duidt erop dat malvertising in de toekomst niet alleen onderdeel zal uitmaken van het arsenaal van doorsnee cybercriminelen, maar mogelijk ook vaker zal worden ingezet in APT's.

Populaire Javascript-bibliotheken bieden aanvallers veel potentie

Het betrekken van externe (Javascript-)bibliotheken in een website heeft de afgelopen periode geleid tot een aantal incidenten (zie het kader Javascript-bibliotheken als hulpmiddel voor digitale aanvallen). Veel websites gebruiken externe Javascript-bibliotheken om eenvoudig functionaliteiten aan een website toe te voegen. Voorbeelden zijn de populaire Javascript-bibliotheken van jQuery en Google Analytics.

Ontwikkelaars van een website verwijzen vaak rechtstreeks naar een Javascript-bibliotheek in plaats van deze bibliotheek te kopiëren naar de eigen website. Dit laatste heeft vanuit beveiligingsoogpunt sterk de voorkeur, omdat de eigenaar van de website zelf de controle behoudt over wat deze aan bezoekers aanbiedt. Wanneer een dergelijke bibliotheek populair is, vormt deze een zeer interessant hulpmiddel voor een aanvaller. Als de aanvaller erin slaagt een Javascript-bibliotheek te manipuleren, dan kan deze vervolgens alle websites aanvallen die dynamisch naar deze bibliotheek verwijzen. Het Javascript-bestand hoeft niet altijd direct aangepast te worden op de server van de maker zelf. Ook het aanpassen van scripts via man-in-the-middle (MitM) aanvallen of het hacken van DNS-records kan effectief zijn.

Het effect van een malafide Javascript is te vergelijken met de effecten van malvertising. In beide gevallen krijgt een grote groep gebruikers in korte tijd een enkel stuk malafide code aangeboden.

Javascript-bibliotheken als hulpmiddel voor digitale aanvallen

Aanvallers van de Syrian Electronic Army (SEA) serveerden een aangepaste versie van een Javascript-bestand van Gigya,[198] een dienst waarmee website-eigenaren socialemediafunctionaliteiten kunnen toevoegen aan hun website. Zij lieten het domein waarop dit bestand werd aangeboden verwijzen naar een eigen server via een DNS-hack. Door de aanpassing kregen gebruikers van diverse websites de melding "You've been hacked by the Syrian Electronic Army (SEA)" te zien.

In het geval van Gigya bleef de schade beperkt tot het tonen van een melding. Dit was begin 2015 niet het geval toen een analyse-script van de Chinese website Baidu in sommige gevallen verwees naar GitHub.[199] Doordat het analyse-script door zeer veel websites gebruikt werd, raakte de website van GitHub overbelast en was de site gedurende een aantal dagen niet of nauwelijks bereikbaar.

Bij een aanval op Afghaanse overheidswebsites werd een veelgebruikt Javascript van deze websites aangepast en aangeboden via een distributienetwerk.[200] Volgens onderzoekers van ThreatConnect zou dit misbruikt worden om bezoekers te infecteren via wateringhole-aanvallen.

Macro's vormen (weer) een populaire aanvalsvector

Recente malware-families als Dridex[201], Vawtrak[202] en Cryptodefense[203] zijn voorbeelden van malware die met behulp van malafide macro's terechtkomen op systemen van eindgebruikers. Het misbruik van Office-macro's door malware is geen nieuw fenomeen. In 1995 was het Concept-virus het eerste virus dat er misbruik van maakte en in 1999 gebruikte het beruchte Melissa-virus macro's om zich verder te verspreiden.[204] Ondanks dat de eerste toepassing ervan dus twintig jaar terug gaat, blijkt het gebruik ervan nog altijd aantrekkelijk.

In het verleden werden macro's ingezet om virussen binnen een netwerk te verspreiden. Tegenwoordig passen kwaadwillenden macro's vooral toe voor het downloaden en installeren van aanvullende malware op een systeem. Een ander belangrijk verschil met de begindagen van macro-malware is dat Office-producten macro's normaal gesproken niet meer automatisch uitvoeren. De aanvallen met macro's gebruiken dan vaak social engineering om de gebruiker te verleiden de ondersteuning van macro's alsnog in te schakelen.[205]

197 http://www.invincea.com/wp-content/uploads/2014/10/Micro-Targeted-Malvertising-WP-10-27-14-1.pdf
198 https://nakedsecurity.sophos.com/2014/11/28/syrian-electronic-army-returns-with-thanksgiving-press-hack/
199 http://arstechnica.com/security/2015/03/github-battles-largest-ddos-in-sites-history-targeted-at-anti-censorship-tools/
200 http://www.threatconnect.com/news/operation-poisoned-helmand/
201 http://blogs.technet.com/b/mmpc/archive/2015/01/02/before-you-enable-those-macros.aspx
202 http://blog.trendmicro.com/trendlabs-security-intelligence/banking-malware-vawtrak-now-uses-malicious-macros-abuses-windows-powershell/
203 http://www.symantec.com/connect/blogs/ransomware-return-macro
204 http://edition.cnn.com/TECH/computing/9903/29/melissa.idg/
205 http://stopmalvertising.com/malware-reports/macro-viruses-a-blast-from-the-past.html

(Draadloze) routers blijken interessante hulpmiddelen voor aanvallers

Aanvallers zijn geïnteresseerd in routers van particulieren en kleine bedrijven voor het uitvoeren van digitale aanvallen, zoals blijkt uit de voorbeelden in het kader Toepassingsmogelijkheden gecompromitteerde routers. Een belangrijke reden hiervoor kan zijn dat deze routers op verschillende manieren zijn aan te vallen. Ook niet-geïnfecteerde systemen binnen het netwerk zijn dan via deze routers toegankelijk en succesvol geïnfecteerde routers bieden diverse toepassingsmogelijkheden voor de kwaadwillende. Er zijn maar weinig gebruikers die de vereiste updates op deze routers installeren, waardoor kwetsbaarheden gedurende langere tijd te misbruiken zijn. Begin 2015 werd bekend dat geïnfecteerde routers als onderdeel van de LizardStresser-service werden ingezet voor het uitvoeren van DDoS-aanvallen.[206]

Conclusie en vooruitblik

Gezien de sterke opkomst van ransomware valt een verdere groei van dit type malware in de toekomst te verwachten. Ransomware richt zich nu met name op traditionele pc's en inmiddels ook smartphones. Door de steeds groeiende connectiviteit van systemen is het echter niet ondenkbaar dat ransomware zich in de toekomst ook gaat richten op andere apparaten die in verbinding staan met het internet. Stel, in de toekomst bestaat de mogelijkheid om een televisie of auto onklaar te maken door deze te infecteren met ransomware. Dan is de kans groot dat een slachtoffer het geëiste bedrag betaalt om weer snel televisie te kunnen kijken of de auto te kunnen starten. Bovendien is het denkbaar dat ransomware ook wordt ingezet voor het frustreren van de bedrijfsvoering van een organisatie.

Actoren gebruiken op dit moment al DDoS-aanvallen om diensten te frustreren. Het is niet altijd duidelijk waarom een actor een dergelijk type aanval uitvoert. De kans bestaat dat criminelen vaker, net als bij ransomware, DDoS-aanvallen gaan inzetten voor financieel gewin. Met een DDoS-aanval gijzelt een crimineel als het ware een deel van de infrastructuur van de organisatie en door geld te vragen voor het stoppen ervan kan een soortgelijk model worden bereikt als bij ransomware. Een voorbeeld van een dergelijke manifestatie die nu al zichtbaar is, is de groep DD4BC. Die dreigt met het uitvoeren van een DDoS-aanval als de organisatie geen bitcoins aan de aanvaller betaalt.[212]

Toepassingsmogelijkheden gecompromitteerde routers

Een gecompromitteerde router is een interessant hulpmiddel voor veel kwaadwillenden. Een greep uit de voorbeelden die afgelopen jaar voorbij kwamen:

- Door het aanpassen van DNS-instellingen op routers is het mogelijk gebruikers in het thuisnetwerk om te leiden naar malafide webpagina's of om hen van malafide updates te voorzien zonder dat het systeem in het netwerk zelf geïnfecteerd is.[207]
- Routers vormen een handig hulpmiddel voor het uitvoeren van DDoS-aanvallen, bijvoorbeeld als de router onderdeel uit maakt van een botnet of als de router een service open heeft staan die misbruikt kan worden voor amplificatie-aanvallen, zoals DNS.[208]
- Een worm kan zich via thuisrouters verspreiden, zoals aangetoond door de Moon-worm.[209]
- De router schermt interne systemen normaal gesproken af, maar als de router is gecompromitteerd, kunnen aanvallers deze bescherming doorbreken. Ze hebben dan bijvoorbeeld toegang tot externe harde schijven die via USB zijn aangesloten op de router.[210]
- Malware op een router kan verkeer ongemerkt manipuleren. Bij stemmen via internet gaat er dan bijvoorbeeld ongemerkt een stem naar een andere kandidaat[211] of er wordt malware geïnjecteerd in inkomend verkeer.

De vraag blijft wanneer malware op mobiele platformen daadwerkelijk tot grote problemen gaat leiden. Deze dreiging bestaat op dit moment wel, maar is vooralsnog beperkt. Het lijkt erop dat de architectuur van mobiele platformen voor criminelen nu nog niet aantrekkelijk is om op grote schaal aan te vallen. Mogelijk is het maken van een trojan voor mobiele platformen op dit moment simpelweg nog te duur en leveren traditionele trojans nog voldoende op. Dit kan een verklaring zijn voor het feit dat er minder fraude wordt waargenomen met de apps van banken.[213]

Er is wel een verklaring waarom het ontwikkelen van een trojan voor mobiele platformen zo duur is in vergelijking met traditionele systemen. Op traditionele systemen gebruiken veel mensen dezelfde browsers waarin ze alle diensten raadplegen. Bij mobiele platformen gebeurt dit via afzonderlijke apps die verschillen qua ontwerp, protocollen en technieken. Om deze apps aan te vallen

206 http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/
207 http://www.cert.pl/news/8019/langswitch_lang/en; https://securelist.com/blog/incidents/66358/web-based-attack-targeting-home-routers-the-brazilian-way/; https://www.proofpoint.com/us/threat-insight/post/Phish-Pharm
208 http://nominum.com/news-post/24m-home-routers-expose-ddos/
209 https://isc.sans.edu/diary/Linksys+Worm+%22TheMoon%22+Summary%3A+What+we+know+so+far/17633
210 http://www.pcworld.com/article/2086280/default-settings-leave-external-hard-drives-connected-to-asus-routers-wide-open.html
211 http://galois.com/wp-content/uploads/2014/11/technical-hack-a-pdf.pdf
212 https://blogs.akamai.com/2015/04/dd4bc-operation-profile-medium-risk.html
213 https://www.security.nl/posting/431645/ING%3A+mobiel+bankieren+apps+niet+interessant+voor+crimineel

zal een aanvaller in veel gevallen een hele gerichte, en dus dure, trojan moeten schrijven voor een specifieke app. Zo lang het dus winstgevender blijft om malware voor traditionele pc's te schrijven, zal de hoeveelheid malware voor mobiele platformen niet snel exploderen.

Tot slot zijn er technieken en aanvalsmethoden die al enige tijd bestaan en ook de komende periode tot problemen zullen blijven leiden. Zo zal spearphishing het middel van diverse actoren blijven om in te breken op de systemen van hun slachtoffers, zal malvertising ingezet blijven om in korte tijd grote groepen gebruikers te infecteren met bijvoorbeeld ransomware, zullen de sporen van digitale aanvallen steeds moeilijker te ontdekken en te herleiden zijn en zullen criminelen hun aanpak in al deze gevallen steeds verder blijven verfijnen.

De cloud bestaat niet, er zijn alleen computers van anderen



4 Weerbaarheid: Kwetsbaarheden

In het afgelopen jaar werd de beeldvorming rondom kwetsbaarheden bepaald door publiciteitscampagnes zoals Heartbleed, voorzien van een naam, logo en website. Hierdoor werd het grote publiek meer bekend met kwetsbaarheden in software. Ook richtte de aandacht zich op de gebruiker als bron van kwetsbaarheid door phishingaanvallen en beveiligingsproblemen van clouddiensten. Kwetsbaarheden in software vormen nog steeds de achilleshiel van security.

Een kwetsbaarheid is een eigenschap van ICT, een organisatie of gebruiker die actoren kunnen misbruiken om hun doelen te bereiken of die door een natuurlijke of technische gebeurtenis kan leiden tot verstoringen. In dit hoofdstuk wordt ingegaan op de ontwikkelingen op het gebied van kwetsbaarheden.

Organisatorische ontwikkelingen

Kwetsbaarheden met publiciteitscampagnes

In de afgelopen rapportageperiode was er veel meer publiciteit rondom technische kwetsbaarheden. Heartbleed, een van de bekendste kwetsbaarheden van 2014, vormde hierbij het startpunt.[214] Door de kwetsbaarheid in OpenSSL konden aanvallers op afstand het interne geheugen van systemen uitlezen. Op het moment dat Heartbleed bekend werd gemaakt, was er door de ontdekkers een volledige website gemaakt, inclusief een gelikt logo. De campagne onderstreepte dat veiligheid van opensource-oplossingen als OpenSSL onder andere afhankelijk is van financiële ondersteuning.

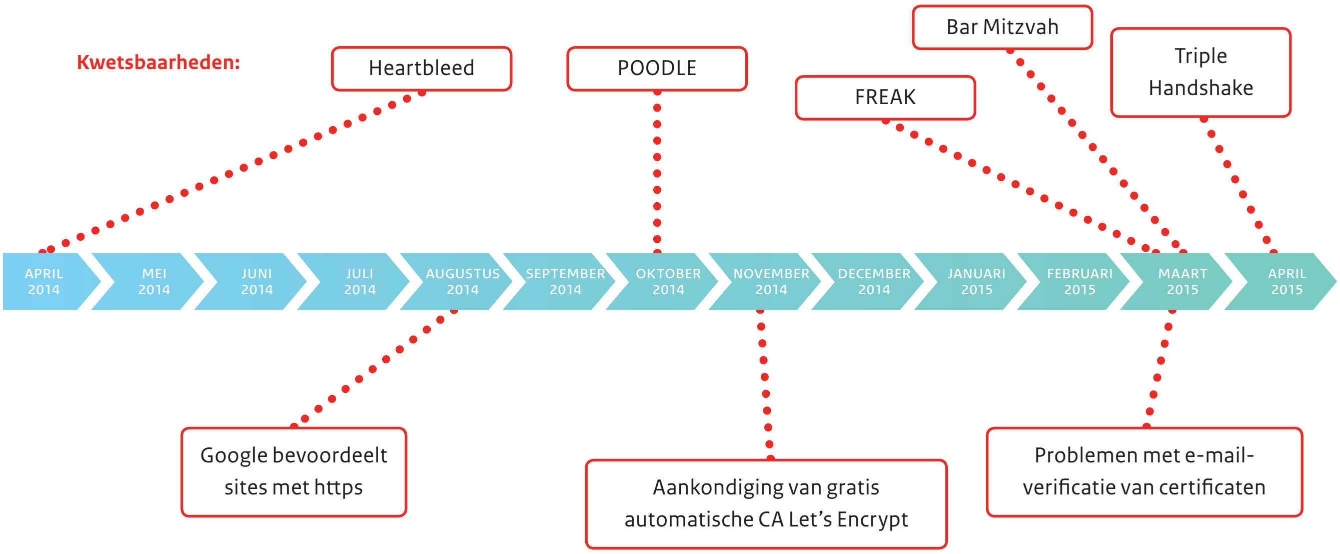
Ook andere kwetsbaarheden werden met vergelijkbare campagnes bekendgemaakt. In september 2014 werd Shellshock,[215] een

214 http://heartbleed.com/
215 https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/
216 Gepubliceerd met toestemming van de maker, Ken Westin.

Figuur 7 **Overzicht van kwetsbaarheden die veel aandacht kregen**[216]



Figuur 8 **Ontwikkelingen rond TLS in het afgelopen jaar**



kwetsbaarheid in de Bash-shell, wereldkundig gemaakt. Shellshock liet aanvallers toe op afstand commando's uit te voeren op geïnfecteerde systemen. Omdat de Bash-shell een belangrijk onderdeel van Linux is, waar veel andere programma's gebruik van maken, had deze kwetsbaarheid een hoge impact.

In oktober 2014 werd POODLE bekend.[217] Deze kwetsbaarheid liet aanvallers toe om in te breken in beveiligde verbindingen die gebruikmaakten van SSLv3. Deze kwetsbaarheid was van tevoren zonder details aangekondigd om updates voor te bereiden, maar dit keer werd alleen een uitgeschreven adviesartikel gepubliceerd en bleven de website en logo achterwege. De kwetsbaarheid liet duidelijk zien dat SSLv3 nu echt niet meer als veilig gezien kan worden en moest worden uitgefaseerd. Ook Linux-kwetsbaarheid GHOST werd in januari 2015 uitgebreid bekendgemaakt. Deze kwetsbaarheid was van tevoren gedeeld met de meeste Linuxdistributies, waardoor de impact beperkt bleef.

De volgende cryptografische kwetsbaarheid, FREAK,[218] werd in maart 2015 bekendgemaakt. Door deze kwetsbaarheid konden aanvallers het beveiligingsniveau van beveiligde verbindingen verlagen. Dit zorgde ervoor dat zwak sleutelmateriaal gebruikt werd voor die verbindingen, die vervolgens zonder veel moeite te kraken waren. De aankondiging werd ondersteund met een website, dit keer zonder logo, en kreeg opnieuw veel publiciteit.

De FREAK-kwetsbaarheid liet zien dat de verzwakking van cryptografie onder druk van exportbeperkingen[219] een lange nasleep kan hebben.

Uit verschillende sectoren komen signalen dat er een risico schuilt in deze publiciteitscampagnes. Door de grote aandacht voor individuele kwetsbaarheden kan de waan van de dag de aandacht afleiden van structurele oplossingen. Bestuurders nemen dan niet altijd beslissingen op basis van de juiste informatie. In de organisaties ontstaat dan het beeld dat de informatiebeveiligers onvoldoende voorbereid zijn.

Het afgelopen jaar hoopten onderzoekers ook voor een aantal andere kwetsbaarheden op eenzelfde golf van publiciteit, maar dat lukte niet. Een voorbeeld is de Triple Handshake,[220] een kwetsbaarheid in het TLS-protocol die het aanvallers mogelijk maakte om in sommige gevallen beveiligde verbindingen af te luisteren. Deze (ingewikkelde) kwetsbaarheid was vrij snel opgelost door de verschillende implementaties.

Een ander voorbeeld was de Bar Mitzvah-aanval[221] die in maart 2015 bekend werd. Deze aanval maakte gebruik van een oude kwetsbaarheid in RC4. Al sinds 2013 is bekend dat deze cryptografische methode erg zwak is.[222 223] Als systemen zijn ingericht om geen gebruik te maken van RC4, zijn ze niet kwetsbaar voor deze aanval.

217 https://www.openssl.org/~bodo/ssl-poodle.pdf
218 https://freakattack.com/
219 http://en.wikipedia.org/wiki/Crypto_Wars
220 https://www.secure-resumption.com/
221 http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf
222 http://www.isg.rhul.ac.uk/tls/
223 https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2013-0208+1.00+Gebruik+RC4+in+TLS+ontraden.html

Cloudinfrastructuur als extensie van het bedrijfsnetwerk

Het toenemende gebruik van clouddiensten stelt gebruikers voor een aantal uitdagingen. Zij moeten zelf beveiligingsmaatregelen nemen. Ook de beveiliging van de infrastructuur van de cloud zelf kan een probleem zijn. Aan de voorkant is niet altijd duidelijk dat aanbieders van bepaalde diensten (achter de schermen) gebruikmaken van clouddiensten, zoals de Amazon-cloud als platform voor mobiele apps. Uit recent onderzoek[224] blijkt dat het gemiddelde bedrijf meer dan 500 cloud-apps gebruikt.

Omdat clouddiensten meer gebruikt worden, moet niet alleen het bedrijfsnetwerk goed worden beveiligd, maar ook de toegang tot clouddiensten en de opslag van data. Verder staan veel van deze 'computers van anderen' niet in Nederland. Dat vergroot het risico op spionage[225] of overtreding van privacywetgeving.[226]

Up-to-date blijven

Kwetsbaarheden in software worden door leveranciers opgelost door het uitbrengen van updates. Als software niet up-to-date is, blijven de kwetsbaarheden aanwezig.[227] Dat komt omdat gebruikers niet voldoende bekend zijn met de noodzaak van updates, of omdat updates conflicten veroorzaken met andere programma's. Uit onderzoek[228] blijkt dat bijna 80 procent van de misbruikte kwetsbaarheden van de meest voorkomende exploitkits meer dan één jaar oud is. Dat oude kwetsbaarheden nog steeds relevant zijn, blijkt ook uit cijfers van de Consumentenbond:[229] 39 procent van de onderzochte computers bevatte verouderde versies van Java, Adobe Flash of Adobe Reader. Ook de contentmanagementsystemen van webpagina's kennen veel kwetsbaarheden.[230]

Het afgelopen jaar is er veel aandacht geweest voor de end-of-life van Windows XP. Na 14 april 2014 zouden er geen updates meer komen voor Windows XP. Volgens statcounter.com[231] halveerde het aantal Nederlandse Windows XP-gebruikers tijdens de rapportageperiode. Nog altijd gebruikt echter 3,1 procent van de Nederlanders Windows XP. De van tevoren aangekondigde 'XPocalypse' (ook in het vorige CSBN genoemd) bleef echter uit.

Bij applicaties en besturingssystemen worden gebruikers nog vaak gewezen op updates, al dan niet via de software zelf. Dat gebeurt bij andere apparaten niet altijd. Zelfs als bij gebruikers bekend is dat updates uitgevoerd moeten worden, is het niet altijd eenvoudig om dit daadwerkelijk te doen. Dit speelt bijvoorbeeld bij thuisrouters, apparaten in het Internet der Dingen[232] en ICS. De beveiliging van deze miljarden apparaten is een bron van grote zorg voor onderzoekers en beveiligers.[233]

Gebruiker als kwetsbaarheid?

Verschillende technische ontwikkelingen lieten het afgelopen jaar zien dat het riskant is om te vertrouwen op gebruikersbewustzijn als basis voor het oplossen van kwetsbaarheden. E-mails met phishingpogingen zijn bijna niet meer van echte e-mails te onderscheiden. De beveiliging van accounts voor webdiensten bleek ook onvoldoende, waardoor veel gevoelige informatie op straat kwam te liggen.

Phishing

Phishing is een bekend onderwerp uit voorgaande edities van het CSBN. Ook dit jaar was deze vorm van social engineering een populaire kwetsbaarheid om uit te buiten. De kwaliteit van de phishingteksten is steeds beter geworden. Het is gebruikers bijna niet meer kwalijk te nemen dat ze erin trappen. Volgens recent onderzoek[234] van Google lokt een goed uitgevoerde phishing-e-mail maar liefst 45 procent van de gebruikers in de val.

Een domeinnaamhouder kan phishing vanaf zijn domein moeilijker maken door het gebruik van de standaarden DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF) en Domain-based Message Authentication, Reporting, and Conformance (DMARC). Legitieme e-mail vanaf zijn domein is dan herkenbaar, waardoor phishing wordt bemoeilijkt. Het gebruik van deze standaarden blijft nog achter: binnen de overheid staat DKIM ingesteld op 10,5 procent van de domeinnamen, SPF op 7,7 procent en DMARC op 4,4 procent.[235] Bij de op internet.nl geteste .nl-domeinen voor e-mail lag dat gebruik hoger. Hier was DKIM ingesteld op 42,1 procent van de domeinen, SPF op 55,6 procent en DMARC op 15,3 procent.[236]

224 https://blog.cloudsecurityalliance.org/2015/04/23/compromised-accounts-and-cloud-activity/
225 Zie ook jaarverslag AIVD 2014.
226 https://cbpweb.nl/sites/default/files/downloads/med/med_20120910-zienswijze-toepassing-wbp-surfmarket-cloud-computing.pdf
227 https://www.security.nl/posting/424028/Ongepatchte+Microsoft+Office+zwakke+plek+Windowsgebruikers
228 http://contagiodump.blogspot.nl/2010/06/overview-of-exploit-packs-update.html
229 http://www.consumentenbond.nl/actueel/nieuws/2015/tweederde-windows-pc-s-heeft-ernstige-beveiligingsproblemen/
230 Zie Hoofdstuk 3 voor details.
231 http://gs.statcounter.com/#desktop-os-NL-monthly-201404-201504
232 Zie ook het katern "Internet der Dingen" in het CSBN-4.
233 Zie bijvoorbeeld http://www.forbes.com/sites/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/
234 http://services.google.com/fh/files/blogs/google_hijacking_study_2014.pdf
235 Meting door internet.nl op 9430 domeinnamen van de overheid, juli 2015.
236 Resultaten van scans door bezoekers van internet.nl op 863 e-maildomeinen, periode april-juli 2015.

Door de toenemende vermenging van zakelijk en privégebruik van apparatuur is het voor organisaties moeilijker om phishing met e-mailfiltering tegen te houden. Phishing-e-mail komt immers ook binnen op privéaccounts. Door het toepassen van bring-your-own-device (BYOD) bedreigt phishing via een omweg toch nog het bedrijfsnetwerk. Meerdere vitale sectoren gaven aan met deze problematiek te worstelen.

Inloggegevens voor de cloud vormen een zwakke schakel

Er worden steeds meer gegevens opgeslagen in de cloud. De toegangsbeveiliging hiervan is daarom steeds belangrijker. In 2014 vestigde de zogenaamde "Fappening" de aandacht op de kwetsbaarheid van traditionele inlogmethoden. Het incident kreeg veel media-aandacht,[237] omdat er veel compromitterende foto's van beroemdheden openbaar waren gemaakt.

De oorzaak van het incident werd in eerste instantie in een technische kwetsbaarheid bij Apple gezocht, omdat een grote hoeveelheid foto's uit Apple iCloud kwam. Later bleek dit iets genuanceerder te liggen; de aanvallers hebben waarschijnlijk gericht informatie verzameld en misbruik gemaakt van zwakke wachtwoordherstelmechanismes om toegang te krijgen tot de foto's.

Dit incident maakte reguliere gebruikers bewuster van de gevaren van het opslaan van gegevens in de cloud. Dit zorgde op zijn beurt bij de producenten van deze programma's tot een grotere bereidheid om actie te ondernemen. De wachtwoordherstelmechanismes van veel clouddiensten zijn in het afgelopen jaar steviger beveiligd. Dit gebeurde vaak door tweefactorauthenticatie in te stellen of door verbeterde controle voordat wachtwoorden gereset kunnen worden.

Technische ontwikkelingen

Ook op technisch gebied ontwikkelden kwetsbaarheden zich. Naast aanvallen op firmware met een grote impact werd een nieuw soort kwetsbaarheid bekend van het mobiele-telefonienetwerk.

Kwetsbaarheden in firmware

Firmware is software die gebruikt wordt in apparaten zoals harde schijven en USB-sticks, maar ook in wasmachines, auto's en andere apparaten. Kwetsbaarheden in firmware kunnen grote gevolgen hebben, maar het is onbekend hoeveel kwetsbaarheden hierin aanwezig zijn. In de rapportageperiode is een aantal kwetsbaarheden bekend geworden in verschillende soorten firmware. Deze ontdekkingen bevestigden dat aanvallen steeds moeilijker te detecteren zijn. Na infectie is het zo goed als onmogelijk om de aanval op het apparaat zelf te detecteren.

In augustus en oktober 2014 werden presentaties gegeven over BadUSB, een kwetsbaarheid in USB-firmware. Door het insteken van een USB-apparaat kan een computer geïnfecteerd worden. Door de nieuwe techniek van BadUSB kan dit gedaan worden zonder dat de gebruiker of antivirussoftware dit opmerkt.

De firmware van harde schijven kan ook misbruikt worden. Dit werd bekendgemaakt in een rapport over de Equation Group. Misbruik van kwetsbaarheden in deze firmware vereist aanzienlijke kennis en heeft een grote impact. De Equation Group misbruikte deze kwetsbaarheden slechts sporadisch, waarschijnlijk alleen bij belangrijke doelwitten.[238] Dit duidt op de grote waarde ervan voor aanvallers.

Computers bevatten zelf ook firmware om op te starten. Ook hierin is een kwetsbaarheid gevonden. In maart 2015 werd bekend dat UEFI-firmware kwetsbaar was. Een aanvaller die deze kwetsbaarheid misbruikte kon malware installeren op het systeem. Firmware omzeilt beveiligingsmechanismen van het besturingssysteem, omdat het op een laag niveau in het systeem werkt. Zelfs na het volledig wissen van de harde schijf kan de infectie voortduren.

Mobieletelefonienetwerk

Ook in het mobieletelefonienetwerk werden kwetsbaarheden gevonden.[239] Providers gebruiken het SS7-protocol om gesprekken aan elkaar door te geven. SS7 bleek te weinig rekening te houden met beveiliging. Het was voor een aanvaller mogelijk om gesprekken en sms-berichten te onderscheppen. Omdat het hier om een tekortkoming van het protocol gaat (en niet om een softwarefout), is het lastig om deze kwetsbaarheid volledig te verhelpen.

Conclusie en vooruitblik

De ontwikkeling van de cloud zet duidelijk door. Dit stelt zowel gebruikers als bedrijven voor een uitdaging. Voor gebruikers is het niet altijd duidelijk dat gegevens in de cloud terechtkomen. De toegangsbeveiliging voor clouddiensten is een aandachtspunt geweest. Veel diensten zijn inmiddels overgegaan op tweefactorauthenticatie. Voor bedrijven is de cloud een uitbreiding van de eigen faciliteiten. Dit betekent dat goed gekeken moet worden naar de toegang tot en opslag van data bij clouddiensten. Een slecht beveiligde cloud vergroot het risico op spionage of een overtreding van de privacywetgeving.

De afgelopen jaren zijn er verschillende campagnes geweest om gebruikers bewust te maken van digitale dreigingen en mogelijke bescherming daartegen. Misbruik van kwetsbaarheden wordt geavanceerder en moeilijker te herkennen. Sommige

237 http://en.wikipedia.org/wiki/2014_celebrity_photo_hack
238 https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf
239 http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/

Ontwikkelingen in beveiliging op de transportlaag

Het gebruik van https biedt voordelen voor alle soorten webdiensten. Het beschermt gebruikers tegen ongewenst meekijken met hun browsegedrag. Daarnaast kan het bescherming bieden tegen wateringhole-aanvallen, omdat de authenticiteit van de inhoud beter gegarandeerd kan worden. Ten slotte is https voor webdiensten aantrekkelijker omdat Google websites met https hoger in de zoekresultaten plaatst.[240] In april 2015 voegde Google zelfs een functie aan de browser Chrome toe om gebruikers te waarschuwen voor websites zonder https.

Het inzetten van encryptie wordt steeds toegankelijker. In november 2014 werd bekend dat medio 2015 een nieuwe gratis certificaatautoriteit, Let's Encrypt, de deuren opent. Let's Encrypt automatiseert het aanvragen en instellen van certificaten. De meeste webdiensten bieden tegenwoordig hun diensten ook aan over https, of schakelen zelfs automatisch over naar een beveiligde verbinding.

Wereldwijd gebruikt 22,1 procent van de populairste websites https.Bij de overheid maakt 19,4 procent van de websites gebruik van https.[241] Van deze websites hanteert 29,4 procent een veilige configuratie op basis van de ICT-beveiligingsrichtlijnen voor TLS van het NCSC. Dat is 5,8 procent van het totaal.

De toename van het gebruik van https zorgt er ook voor dat andere risico's afnemen. Er wordt al jaren gewaarschuwd voor de risico's van open draadloze netwerken. Als al het webverkeer op de juiste manier gebruikmaakt van https, dan is het veel moeilijker om gebruikers van open draadloze netwerken aan te vallen.

Phishing-e-mails zijn zo nauwgezet opgesteld dat het gebruikers niet altijd kwalijk te nemen is dat ze erin trappen.

De beveiliging van onderliggende infrastructuur verdient ook de aandacht. Kwetsbaarheden in firmware van apparaten zorgen ervoor dat op een laag niveau beveiligingsrisico's ontstaan, die erg moeilijk zijn te detecteren.

240 http://googlewebmastercentral.blogspot.nl/2014/08/https-as-ranking-signal.html
241 Meting door internet.nl op 9430 domeinnamen van de overheid, juli 2015.

Door dreigingsinformatie te delen kunnen organisaties met minder inspanning een completer beeld van de (potentiële) dreigingen krijgen.



5 Weerbaarheid: Maatregelen

Bewust inzetten van technische en niet-technische maatregelen zorgt voor meer bekwaamheid. In de financiële sector waren de genomen maatregelen effectief: ze leidden er bijvoorbeeld toe dat dat bepaalde aanvallen niet of minder voorkomen, of niet meer tot schade leiden. Er zijn echter ook dreigingen die moeilijker te bestrijden zijn. Door nieuwe kwetsbaarheden moeten maatregelen voortdurend worden bijgesteld.

Dit hoofdstuk gaat in op maatregelen die de weerstand en veerkracht van individuen, organisaties en de samenleving versterken en menselijke en technische kwetsbaarheden beperken. Maatregelen kunnen preventief of reactief van aard zijn en zijn gericht op de mens of op de systemen (techniek).

De mens

Thuisgebruikers, werknemers, werkgevers en ondernemers kunnen de weerbaarheid zowel positief als negatief beïnvloeden. De mate waarin men zich bewust is van de aanwezige belangen, kwetsbaarheden en dreigingen en de manier waarop men omgaat met de risico's die hiermee samenhangen, spelen hierin een cruciale rol. Naast bewuste en bekwame gebruikers moeten er bovendien voldoende professionals zijn die de continue stroom kwetsbaarheden verhelpen. Zij kunnen oplossingen aandragen waarmee we ons beter beschermen tegen de steeds geavanceerdere dreigingen.

Bewuste en bekwame gebruikers gedragen zich veiliger

In februari 2015 publiceerde de Europese Commissie de Eurobarometer 2014, een onderzoeksrapport over de publieke opinie over cybersecurity in de 28 EU-lidstaten.[242] De Nederlandse respondent zegt goed op de hoogte te zijn van de risico's van cybercrime (67 procent versus een EU-gemiddelde van 47 procent). De zorgen van Nederlandse respondenten over internetgebruik wijken niet erg af van die van respondenten uit andere lidstaten. Wel passen ze vaker hun internetgebruik aan. Zo hebben meer Nederlandse respondenten antivirussoftware geïnstalleerd (82 procent versus een EU-gemiddelde van 61 procent) en zeggen Nederlandse respondenten vaker geen e-mails te openen van mensen die zij niet kennen (71 procent versus een EU-gemiddelde van 49 procent). Ook zijn Nederlandse respondenten minder geneigd om persoonlijke informatie in te voeren op websites (65 procent versus een EU-gemiddelde van 38 procent) en gebruiken ze vaker verschillende wachtwoorden voor verschillende websites (58 procent versus een EU-gemiddelde van 31 procent).[243]

In de afgelopen periode werd in Nederland op verschillende manieren aandacht gevraagd voor cybersecurity, zowel breed als op specifieke onderwerpen. Vaak gebeurt dit tijdens (inter)nationale campagnes, zoals de Europese Cyber Security Month[244], Alert Online[245], 'Hang op, klik weg, bel uw bank'[246] en Safer Internet Day[247].

Organisaties hebben moeite voldoende cybersecurityprofessionals aan te trekken

'De' cybersecurityprofessional bestaat niet. Cybersecurity is een complex onderwerp, dat vanuit verschillende disciplines (bijvoorbeeld computer-, gedrags- en rechtswetenschappen) moet

242 http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf
243 http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_fact_nl_nl.pdf
244 http://cybersecuritymonth.eu/
245 https://www.alertonline.nl/
246 https://www.veiligbankieren.nl/
247 https://www.saferinternetday.nl/

'Hang op, klik weg, bel uw bank'

Terwijl de totale schade door fraude met internetbankieren in 2014 meer dan halveerde ten opzichte van het jaar ervoor (van 9,6 miljoen euro in 2013 naar 4,7 miljoen euro in 2014), daalde de schade door phishing 'slechts' van 4,7 miljoen euro naar 3,9 miljoen euro.[248] Dit is een reden voor de banken om aandacht voor dit onderwerp te blijven vragen, onder meer tijdens de campagne 'Hang op, klik weg, bel uw bank'. In een aantal landelijke radio- en televisiecommercials en op de bijbehorende website wordt uitgelegd hoe de gebruiker zich kan wapenen tegen phishing, social engineering en andere vormen van fraude met internetbankieren.[249]

worden benaderd.[250] Sommige functies zijn specifiek op cybersecurity gericht, bij andere functies is cybersecurity slechts een onderdeel. Daarnaast kan het oriëntatieniveau van de functies variëren: strategisch, tactisch en/of operationeel.

Meerdere universiteiten bieden masteropleidingen cybersecurity aan

In 2015 zijn drie universitaire masteropleidingen cybersecurity van start gegaan. De Cyber Security Academy, een samenwerkingsverband tussen de Universiteit Leiden, de Technische Universiteit Delft en de Haagse Hogeschool is in januari 2015 gestart met de executive masteropleiding Cyber Security. De TU Delft en Universiteit Twente starten in september 2015 met het 3TU Cyber Security-masterprogramma. Tegelijkertijd start de TRU/e Master in Cyber Security aan de Radboud Universiteit en de TU Eindhoven. De 3TU- en TRU/e-programma's zijn het vervolg van het Kerckhoffs Institute, dat sinds 2006 een gespecialiseerd masterprogramma in cybersecurity bood. Ook de master System and Network Engineering van de Universiteit van Amsterdam, die al sinds 2003 bestaat, is een bekende vooropleiding voor cybersecurityprofessionals.

Wereldwijd is veel aandacht voor de kloof tussen de vraag naar en het aanbod van cybersecurityprofessionals. Uit een enquête onder meer dan drieduizend business- en IT-professionals wereldwijd bleek dat 86 procent van hen gelooft dat er een tekort is aan bekwame cybersecurityprofessionals.[251] In het security-jaarrapport 2014 van Cisco wordt gesproken over een tekort van meer dan één miljoen professionals wereldwijd.[252] In diverse landen, waaronder de Verenigde Staten[253] en Nederland, is arbeidsmarktonderzoek naar cybersecurityprofessionals verricht.

Het onderzoek naar vraag en aanbod van cybersecurityprofessionals in Nederland is in opdracht van het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC) uitgevoerd door PLATO en Ockham IPS.[254] Uit het onderzoek blijkt dat de vraag naar professionals in de komende vijf jaar wel zal stijgen, maar dat het aanbod getalsmatig voldoende is om aan de vraag te voldoen. Op dit moment kunnen vraag en aanbod elkaar echter niet goed vinden. Hoewel er voldoende studenten deelnemen aan relevante opleidingen, stromen er te weinig studenten door naar specifieke cybersecurityfuncties en is de aansluiting van onderwijs op de arbeidsmarkt onvoldoende.

De techniek

Hoewel de mens vaak wordt aangeduid als de zwakste schakel in de cybersecurityketen, is ook de techniek onmisbaar voor het borgen van cybersecurity. In deze paragraaf wordt ingegaan op de belangrijkste ontwikkelingen op dit gebied uit afgelopen periode.

Tweefactorauthenticatie wordt populair

De meestgebruikte manier om toegang te krijgen tot een account is door middel van een gebruikersnaam en wachtwoord. Deze techniek wordt al decennialang gebruikt. Gebruikers kiezen vaak voor simpele wachtwoorden die gemakkelijk te onthouden zijn. Kwaadwillenden kunnen hierdoor makkelijker toegang te krijgen tot accounts. Steeds meer websites ondersteunen tweefactorauthenticatie.[255] Deze techniek voorkomt dat een aanvaller door phishing of het raden van het wachtwoord toegang kan krijgen tot een account. Een voorbeeld van tweefactorauthenticatie is het DigiD-authenticatieniveau DigiD Midden. Daarbij ontvangt een burger na het inloggen met gebruikersnaam en wachtwoord ook een sms met een verificatiecode. Het gebruik van DigiD Midden is in 2014 met 32,7 procent gegroeid ten opzichte van 2013. 80 procent van de DigiD-gebruikers kan inmiddels gebruikmaken van DigiD Midden.[256]

248 http://www.betaalvereniging.nl/wp-uploads/2015/03/150318-Fraude-betalingsverkeer-gehalveerd-20141.pdf
249 https://www.veiligbankieren.nl/nl/nieuws/nieuwe-campagne-veilig-bankieren_hang-op_klik-weg_bel-uw-bank_.html
250 https://www.salve.edu/sites/default/files/filesfield/documents/Professionalizing-Cybersecurity.pdf
251 http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf
252 http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
253 http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf en https://www.salve.edu/sites/default/files/filesfield/documents/Professionalizing-Cybersecurity.pdf
254 http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2015/05/02/tk-bijlage-eindrapport-arbeidsmarkt-cybersecurity-professionals.html
255 Een overzicht is te vinden op https://twofactorauth.org/.
256 https://zoek.officielebekendmakingen.nl/kst-31200-III-3-b1.pdf

Werven in cybersecurity: veel vacatures, weinig mensen

De arbeidsmarkt voor cybersecurityprofessionals kenmerkt zich al langer door een groot verschil tussen de vraag naar en het aanbod van (technische) cybersecurityprofessionals. Het aantal vacatures neemt toe. Organisaties hebben regelmatig moeite om vacatures te vervullen. Dat geldt in het bijzonder voor technische cybersecurityfuncties.

Ook de overheid heeft de afgelopen periode nieuwe medewerkers op dit terrein geworven.

- Team High Tech Crime (THTC) heeft opnieuw een Cybercrime Challenge georganiseerd en eind 2014 is de geplande capaciteitsuitbreiding naar 119 fte gerealiseerd.[257] Ook de regionale eenheden zijn gestart om met 100 digitaal experts uit te breiden.
- Het team dat zich bezighoudt met high tech crime bij het Landelijk Parket van het Openbaar Ministerie is uitgebreid van vier naar zeven fte.[258]
- Defensie heeft het Defensie Cyber Expertise Centrum en het Defensie Cyber Commando opgericht. Het Defensie Cyber Expertise Centrum zorgt voor ontwikkeling, borging en verspreiding van kennis over cybersecurity binnen Defensie.[259] Het groeit naar 18 fte. Het Defensie Cyber Commando zorgt ervoor dat cybersecurity wordt geïntegreerd in militaire operaties en dat offensieve cybercapaciteiten worden ontwikkeld.[260] Voor het Defensie Cyber Commando zijn zestig nieuwe medewerkers aangetrokken.[261]
- In juni 2014 is de Joint Sigint Cyber Unit van de AIVD en MIVD van start gegaan. De gezamenlijke eenheid verricht werkzaamheden ter ondersteuning van de AIVD en de MIVD bij de uitoefening van (bijzondere) bevoegdheden op het gebied van signals intelligence (Sigint) en Cyber. Sigint staat voor inlichtingen die worden verzameld uit (tele)communicatie. Cyber wordt gebruikt als verzamelnaam voor verschillende activiteiten die te maken hebben met computernetwerken en datastromen.[262]
- Het NCSC is sinds 1 januari 2015 gestart met het Nationaal Cyber Security Operations Center (NCSOC), dat 24 uur per dag en 7 dagen in de week als meldpunt fungeert, nieuwe dreigingen en kwetsbaarheden signaleert en zijn netwerk voorziet van informatie.[263] Deze start is samengegaan met een personele uitbreiding.

Cryptografie speelt een sleutelrol in technische beveiliging

Met cryptografische protocollen kan informatie worden versleuteld. Doorgaans wordt dit toegepast wanneer de informatie over een netwerk wordt verzonden of wordt opgeslagen. Verschillende kwetsbaarheden in cryptografische toepassingen (waaronder Heartbleed, POODLE en FREAK) hebben ertoe geleid dat apparaten van updates moesten worden voorzien en dat sleutels en certificaten vervangen moesten worden.

Transport Layer Security (TLS) is een protocol voor het opzetten en gebruiken van een cryptografisch beveiligde verbinding tussen twee computersystemen, bijvoorbeeld een client en een server. TLS wordt gebruikt in diverse toepassingen, waaronder webverkeer (https), e-mailverkeer (IMAP en SMTP over STARTTLS) en bepaalde typen virtual private network (VPN). Er zijn verschillende configuratie-opties voor TLS en lang niet alle opties zijn veilig. Van de op internet.nl geteste websites met .nl-domeinnamen gebruikte 13,7 procent een veilige TLS-configuratie op basis van de ICT-beveiligingsrichtlijnen voor TLS van het NCSC.[264]

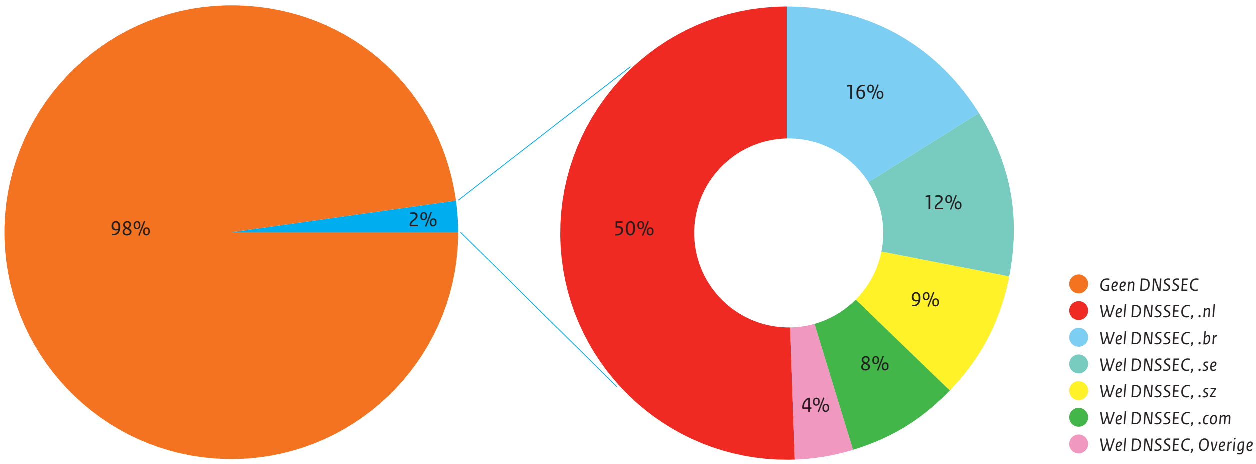
DNS Security Extensions (DNSSEC) is een cryptografische beveiliging voor het DNS-protocol.[265] Sinds 15 mei 2012 kunnen alle .nl-domeinnamen worden voorzien van DNSSEC. DNS is altijd kwetsbaar geweest voor kwaadwillenden. Daardoor ontstaat de kans dat internetgebruikers op een malafide website terechtkomen, terwijl de gebruikte domeinnaam juist is. Bij gebruik van DNSSEC wordt gecontroleerd of het gegeven antwoord authentiek is en afkomstig is van de juiste bron. Gebruikers kunnen dus verifiëren of ze op de juiste website zijn. Dit vergroot de betrouwbaarheid van het DNS. Het gebruik van DNSSEC is in de afgelopen periode gegroeid met 12 procent: ruim 43 procent van de .nl-zone is inmiddels beschermd.[266] Voor de overheid ligt dat percentage lager: 7,8 procent van de domeinnamen van de overheid is met DNSSEC beschermd.[267] De helft van alle met DNSSEC beschermde domeinnamen wereldwijd eindigt op .nl. Daarmee loopt Nederland in absolute aantallen ruimschoots voorop.

Detectiecapaciteit is essentieel om geavanceerde aanvallen te ontdekken

Eerdere DDoS-aanvallen hebben geleid tot meer detecterende en mitigerende maatregelen. De maatregelen die in de financiële sector worden genomen tegen DDoS-aanvallen blijken effectief.

257 Jaarverslag Eenheid Den Haag 2014, via http://www.regioburgemeesters.nl/regio/6-den-haag/.
258 http://www.tweedekamer.nl/kamerstukken/detail?id=2015D04792
259 http://www.vovklict.nl/intercom/2014/3/33.pdf
260 http://www.defensie.nl/actueel/nieuws/2014/09/25/minister-geeft-startschot-voor-defensie-cyber-commando
261 https://tweakers.net/nieuws/98679/minister-van-defensie-opent-cyber-commando-krijgsonderdeel.html
262 https://www.aivd.nl/publicaties/@3115/joint-sigint-cyber/
263 https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/24-uurs-hulp.html
264 Resultaten van scans door bezoekers van internet.nl op 3067 domeinnamen, periode april-juli 2015.
265 http://dnssec.nl/wat-is-dnssec/overzicht.html
266 https://stats.sidnlabs.nl/
267 Meting door internet.nl op 9430 domeinnamen van de overheid, juli 2015.

Figuur 9 **Gebruik van DNSSEC op domeinnamen wereldwijd en onder specifieke topleveldomeinen**



Links: wereldwijde verhouding wel/geen DNSSEC. Rechts: opbouw van domeinnamen die wel DNSSEC gebruiken.[268]

Inperken van cryptografie

Omdat cryptografie de opsporing kan bemoeilijken, pleiten sommige overheden ervoor om de toepassing ervan in te perken. Deze wens bestaat al langer: de Verenigde Staten hebben bijvoorbeeld in de jaren negentig de export van sterke cryptografie aan banden gelegd.[269] In januari 2015 laaide de discussie opnieuw op, ook in Nederland, toen de premier van het Verenigd Koninkrijk David Cameron tijdens een persconferentie zei dat hij vanwege nieuwe anti-terreurmaatregelen wil dat communicatiediensten die met end-to-end-encryptie werken (zoals WhatsApp) worden verboden. Volgens Cameron moeten geheime diensten altijd toegang tot de inhoud van deze communicatie kunnen krijgen.[270] Tegenstanders van een dergelijke inperking wijzen vooral op het belang van cryptografie voor digitale veiligheid, privacy en economische activiteit. Zij betwijfelen de haalbaarheid en effectiviteit van een dergelijk verbod.[271]

DDoS-aanvallen veroorzaken nauwelijks problemen meer in de financiële sector. Geavanceerdere aanvallen zoals Advanced Persistent Threats (APT's) zijn een ander verhaal. Deze aanvallen, die gericht zijn op organisaties in verschillende sectoren, omzeilen structureel bestaande beveiligingsmaatregelen en zijn zeer moeilijk te detecteren. De aanvallen blijven vaak maanden tot jaren onopgemerkt. Dit kan leiden tot grote en ingrijpende schade voor de getroffen organisaties. Permanent van een aanval afkomen is ook lastig. De AIVD heeft meermaals waargenomen dat aanvallers bij detectie en verwijdering van de initiële malware al snel op een andere wijze hetzelfde doelwitnetwerk binnendrongen.[272] Hoewel steeds meer organisaties speciale software hebben tegen APT's, lijkt het weren ervan voor veel organisaties een grotendeels onontgonnen gebied. De vele rapporten over APT's die in de afgelopen periode gepubliceerd zijn[273] kunnen wel helpen om meer inzicht te krijgen in de werking van APT's en daarmee met het bepalen van maatregelen.

Ook beveiliging van opensourcesoftware kost geld

De Heartbleed-kwetsbaarheid[274] maakte duidelijk dat opensourcesoftware niet automatisch veiliger is, zelfs als die veel gebruikt wordt. De OpenSSL-bibliotheek bevatte een bug die pas na enkele jaren werd opgemerkt. De publiciteit rond deze bug leidde er in april 2014 toe dat grote internetbedrijven de handen ineen sloegen in het Core Infrastructure Initiative. Met deze samenwerking wordt geïnvesteerd in de opensource-basisinfrastructuur van het internet.

Het initiatief stelt geld beschikbaar om opensourcesoftware-projecten, zoals OpenSSL, te ondersteunen. Ook OpenSSH en NTP worden nu ondersteund. Dit initiatief verbetert de basisbeveiliging van het internet. Het bestrijkt echter momenteel slechts een klein deel van de opensource-projecten die de infrastructuur van het internet dragen. Voor andere projecten is minder financiering beschikbaar.

268 Analyse op basis van gegevens van http://rick.eng.br/dnssecstat/ en https://www.verisigninc.com/assets/domain-name-report-march2015.pdf.
269 Zie bijvoorbeeld: http://www.heise.de/tp/artikel/2/2898/1.html.
270 http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror
271 Zie bijvoorbeeld: http://dspace.mit.edu/handle/1721.1/97690.
272 https://www.aivd.nl/@3247/jaarverslag-aivd/
273 Zie bijvoorbeeld APTnotes, een openbare lijst van APT-rapporten: https://github.com/kbandla/APTnotes.
274 Zie Hoofdstuk 4 Weerbaarheid: Kwetsbaarheden.

Responsible disclosure

Het aantal organisaties in Nederland dat een responsible-disclosurebeleid (RD) hanteert groeit nog steeds.[275] Binnen en buiten de vitale sectoren is door veel individuele en samenwerkende partijen gewerkt aan het opstellen van een eigen RD-beleid. Ook zijn er websites gelanceerd en discussiesessies georganiseerd om RD te bevorderen. In 2014 zijn 120 bruikbare meldingen binnengekomen bij het meldpunt responsible disclosure van telecombedrijven. In 2013 waren dat er 77. Het NCSC heeft in de afgelopen periode ruim 150 RD-meldingen afgehandeld. Zie ook de paragraaf Responsible Disclosure in Bijlage 1.

Ethische hackers plaatsen soms kanttekeningen bij RD, omdat zij vinden dat vervolging niet mogelijk zou moeten zijn. Het toenemend aantal meldingen wijst echter op het groeiend vertrouwen tussen de bredere ICT-community, de overheid en het bedrijfsleven.[276] Het Openbaar Ministerie heeft in de afgelopen periode ook geen vervolging ingesteld naar melders die conform het RD-beleid van de desbetreffende organisaties handelden.[277]

Samenwerking

In Nederland bestaan vele samenwerkingsverbanden die tot doel hebben de digitale weerbaarheid te versterken. In deze paragraaf worden enkele van deze initiatieven toegelicht.

Fraude met behulp van malware wordt met succes teruggedrongen

Ondanks de voortdurende sterke groei van het internetbankieren, daalde de schade door malware bij Nederlandse banken met 90 procent tot minder dan 500.000 euro.[278] Interbancaire detectiesystemen (zoals de Cybercrime Monitoring & Investigation Services) kunnen fraude met malware steeds beter automatisch detecteren en voorkomen. De Nederlandse banken zijn waarschijnlijk succesvol, omdat zij niet concurreren op veiligheid.[279] Volgens de Betaalvereniging Nederland en de Nederlandse Vereniging van Banken is goede samenwerking de sleutel tot het veilig houden van het betalingsverkeer.[280]

Skimming komt nagenoeg niet meer voor

Het skimmen van betaalpassen is in 2014 fors teruggedrongen. De schade door skimmen is met 82 procent gedaald naar minder dan 1,3 miljoen euro in 2014.[280] Het skimmen is niet meer aantrekkelijk voor fraudeurs door de invoering van de EMV-betaalchip op alle betaalpassen, het 'geoblocken' van pinnen buiten Europa en extra antiskimmingmaatregelen op onbemande betaal- en geldautomaten. De laatste keer dat iemand in Nederland werd geskimd bij een bemande betaalautomaat aan de toonbank was in 2012. Bij een geldautomaat gebeurde dit eind 2013 voor het laatst.[280]

Strijden tegen botnets: neerhalen en data delen

In juni 2014 haalden de FBI, Europol, verschillende commerciële (security)bedrijven en onderzoekers van de Vrije Universiteit het beruchte GameOver Zeus-botnet uit de lucht.[281] Deze Operation Tovar trok veel publiciteit en leidde tot de arrestatie van verschillende personen. Een maand later berichtten de UK National Crime Agency en Europol over het neerhalen van het Shylock botnet.[282] Hoewel het neerhalen van botnets veel media-aandacht krijgt, verschijnen kort erna vaak berichten die het succes in twijfel trekken. Na het GameOver Zeusbotnet was er al snel een gewijzigde vorm van het botnet actief. Bovendien zijn er verschillende botnets (waaronder sommige die van Zeus afstammen) die het gat opvullen dat GameOver Zeus achterliet. Hoewel het noodzakelijk blijft om individuele botnets aan te pakken, is het dus nog maar de vraag of met deze aanpak de algehele botnetproblematiek wordt verkleind.

De Vereniging Abuse Information Exchange is een initiatief van KPN, SIDN, Solcon, Tele2, UPC, XS4ALL, Zeelandnet en Ziggo. De vereniging vertegenwoordigt meer dan 90 procent van de markt van Nederlandse internetproviders en heeft tot doel de informatievoorziening over botnets en andere vormen van internetmisbruik in Nederland te verbeteren. Ze verzamelen en correleren data over besmettingen uit verschillende bronnen op één centraal punt. Botnetbesmettingen kunnen zo sneller en beter worden bestreden, zodat de veiligheid en stabiliteit van het internet worden verbeterd. Dit systeem, AbuseHUB, werd in juni 2014 officieel in gebruik genomen.[283]

Delen van dreigingsinformatie helpt om capaciteit efficiënt in te zetten

De behoefte aan oplossingen op het gebied van monitoring stijgt. Door continu de systemen en applicaties in het netwerk in de gaten te houden (monitoring) kunnen dreigingen vroegtijdig worden gesignaleerd (detectie) en kan snel worden ingegrepen wanneer daadwerkelijk iets gebeurt (respons). Hierdoor kan de schade beperkt

275 Kamerbrief over voortgang responsible disclosure, http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/12/19/tk-voortgang-responsible-disclosure.html.

276 https://www.ncsc.nl/actueel/nieuwsberichten/responsible-disclosure-steeds-breder-toegepast.html

277 http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/12/19/tk-voortgang-responsible-disclosure.html

278 http://www.betaalvereniging.nl/wp-uploads/2015/03/150318-Fraude-betalingsverkeer-gehalveerd-20141.pdf

279 http://fd.nl/economie-politiek/1102338/aanpak-cybercrime-bij-banken-wordt-exportproduct

280 http://www.betaalvereniging.nl/nieuws/fraude-met-internetbankieren-gehalveerd

281 https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted

282 https://kcdp.ncsc.nl/Global%20action%20targeting%20Shylock%20malware.pdf

283 https://www.abuseinformationexchange.nl/

Nederland Schoon

Nederland is niet alleen een direct doelwit, maar is ook een grote doorvoerhaven voor digitale aanvallen.[284] Nederland staat wereldwijd bekend als belangrijk hostingland van digitale data, onder meer vanwege de stabiele netwerken, hoge bandbreedtes en relatief lage kosten. De aanwezigheid van één van de grootste internetknooppunten ter wereld en een professionele en volwassen hostingbranche dragen ook bij aan deze reputatie. Deze omstandigheden trekken activiteiten aan vanuit de hele wereld. Het gaat primair om bonafide activiteiten, maar helaas soms ook om minder bonafide. Daardoor is Nederland bovengemiddeld vaak een uitvalsbasis voor uiteenlopende vormen van cybercrime, zoals het verspreiden van malware, het versturen van phishing- en spamberichten en het stallen van gestolen data.

Om nationaal en internationaal verantwoordelijkheid te nemen als hostingland startten de politie, de Autoriteit Consument en Markt, het Openbaar Ministerie en de TU Delft in 2014 het project Nederland Schoon. Dit project heeft als doel om cybercrime vanuit die infrastructuren aan te pakken in nauwe samenwerking met de branche zelf. Nederland Schoon gaat de komende tijd verschillende acties uitvoeren.

In samenwerking met de TU Delft is in kaart gebracht welke hostingproviders door cybercriminelen worden gebruikt. Veel hostingbedrijven zijn al goed op weg om cybercrime tegen te gaan. Sommige hostingproviders spelen een faciliterende rol bij cybercrime. Het kan zijn dat hostingbedrijven zich niet bewust zijn van hun faciliterende rol. Vanuit het project wordt daarom onder andere in gesprek gegaan met hostingproviders die volgens de meting van de TU Delft hoger scoren dan hun branchegenoten.

worden. Monitoring is echter arbeids- en kostenintensief. Het is niet voor elke organisatie haalbaar om hier 24 uur per dag en 7 dagen per week personeel voor in te zetten.[285] Door dreigingsinformatie te delen kunnen organisaties met minder inspanning een completer beeld van de (potentiële) dreigingen krijgen en hier op reageren. Hiervoor zijn onder andere de standaarden STIX[286] en TAXII[287] beschikbaar.

Een voorbeeld van samenwerking voor het delen van dreigingsinformatie is het Nationaal Detectie Netwerk (NDN). Het NDN is een Nederlands publiek-privaat netwerk gericht op het beter en sneller waarnemen van digitale gevaren en risico's. Door het delen van dreigingsinformatie kunnen partijen vanuit de eigen verantwoordelijkheid tijdig maatregelen nemen om mogelijke schade te beperken of voorkomen.[288]

Oefeningen helpen bij voorbereiden respons

In de afgelopen periode hebben diverse (inter)nationale oefeningen plaatsgevonden. Op 28 april 2014 deden meer dan 200 organisaties en 400 cybersecurityprofessionals uit heel Europa, waaronder Nederland, mee aan ENISA's Cyber Europe oefening.[289] In oktober 2014 vond CyberDawn plaats, gericht op de samenwerking van telecombedrijven, vitale sectoren en de overheid bij grote digitale aanvallen.[290] Door mee te draaien in dergelijke oefeningen leren medewerkers en organisaties wat zij moeten en kunnen doen bij (dreigende) incidenten.

Regulering

Het wetsvoorstel voor de meldplicht datalekken werd op 10 februari 2015 met algemene stemmen aangenomen door de Tweede Kamer.[291] De voorgestelde meldplicht wil datalekken door inbreuken op de beveiliging voorkomen en als deze zich toch voordoen, de gevolgen ervan voor de betrokkenen zoveel mogelijk beperken.[292] Bij een inbreuk waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op verlies of onrechtmatige verwerking van persoonsgegevens moet de verantwoordelijke (zowel in de private als publieke sector) een melding doen bij de toezichthouder, het College bescherming persoonsgegevens én aan de betrokkene. Het niet melden van een datalek kan bestraft worden met een bestuurlijke boete.

In de afgelopen periode is ook op verschillende manieren aandacht besteed aan het gebruik van normen, standaarden, richtlijnen en good practices die organisaties hanteren om de weerbaarheid te verhogen. Uit een onderzoek van ISACA blijkt dat veel organisaties wel een uitgebreid cybersecuritybeleid hebben en daarbij normen en standaarden hanteren, maar dat het snel veranderende dreigingslandschap ervoor zorgt dat de dekking ervan niet altijd volledig is.[293] Voor bestuurders is hier een belangrijke rol weggelegd, omdat zij op strategisch niveau continu de kaders dienen te bepalen voor het formuleren, implementeren, bewaken en handhaven van het cybersecuritybeleid. De Cyber Security Raad

284 https://www.aivd.nl/@3247/jaarverslag-aivd/
285 Capgemini, Rapport Trends in Veiligheid 2014, http://www.trendsinveiligheid.nl/publicaties2014.
286 https://stix.mitre.org/
287 https://taxii.mitre.org/
288 https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/het-nationaal-detectie-netwerk.html
289 https://www.enisa.europa.eu/media/press-releases/biggest-eu-cyber-security-exercise-to-date-cyber-europe-2014-taking-place-today
290 http://www.nederlandict.nl/index.shtml?id=13663&ch=ICT
291 http://www.eerstekamer.nl/wetsvoorstel/33662_meldplicht_datalekken_en
292 http://www.eerstekamer.nl/behandeling/20130617/memorie_van_toelichting_4/document3/f=/vjc76lpx9ryk.pdf
293 https://isaca.nl/dmdocuments/ISACA-survey2014.pdf

heeft voor bestuurders een handreiking opgesteld om ze hierin te ondersteunen.[297]

Het Platform Internetstandaarden, een samenwerkingsverband met partijen uit de internetgemeenschap en de Nederlandse overheid, heeft als doel het gebruik van moderne internetstandaarden (zoals IPv6, DNSSEC, TLS, DKIM, SPF en DMARC) te stimuleren en daarmee het internet voor iedereen betrouwbaarder maken.[298] In april 2015 heeft het platform de website internet.nl gelanceerd.[299] Op deze website kunnen bezoekers eenvoudig nagaan of hun internetverbinding, hun e-mail en de websites die ze bezoeken wel moderne, veilige internetstandaarden hanteren.

Conclusie en vooruitblik

De overheid en het bedrijfsleven investeren flink in de bescherming van de belangen en de versterking van de digitale weerbaarheid van individuen, organisaties en de samenleving. Er lopen meer weerbaarheidsinitiatieven in Nederland dan in dit hoofdstuk zijn beschreven. Er is aandacht voor de menselijke factor (met de noodzaak van bewuste en bekwame gebruikers aan de ene kant en van professionals aan de andere kant), voor de technologische middelen en voor de samenwerking met anderen om uitdagingen beter het hoofd te kunnen bieden.

Er zijn weinig cijfers en statistieken beschikbaar over de maatregelen die organisaties treffen. Organisaties zijn begrijpelijkerwijs terughoudend bij het delen van informatie over hun maatregelen, omdat die informatie actoren in de kaart kan spelen. Een overkoepelend beeld van de getroffen maatregelen is hierdoor moeilijk te geven. Dat maakt het lastig een inschatting te geven van het actuele weerbaarheidsniveau.

Investeren in maatregelen en samenwerking loont zeker, maar is nog niet in alle gevallen effectief. Voor bepaalde dreigingen, zoals botnets en APT's, lijken de juiste maatregelen nog niet te zijn gevonden. Organisaties moeten zich ervan bewust zijn dat het snel veranderende dreigingslandschap ertoe leidt dat de dekking van hun cybersecuritybeleid niet altijd volledig is. Het is daarom van belang dat zij hun beleid en maatregelen regelmatig herzien. Doordat aanvallen geavanceerder worden en steeds lastiger zijn te herkennen, blijft bewustwording belangrijk. Monitoring, detectie en respons zijn ook essentieel, niet in de laatste plaats omdat actoren continu naar manieren zoeken om bestaande beveiligingsmaatregelen te omzeilen.

Afschaffing bewaarplicht telecommunicatiegegevens

Buiten de nieuwe wetten die in de maak zijn, is er in Nederland in de afgelopen periode ook een wet buiten werking gesteld: de Wet bewaarplicht telecommunicatiegegevens. Deze wet werd in 2009 ingevoerd en was gebaseerd op de EU-richtlijn Dataretentie. De wet moest ervoor zorgen dat telecommunicatiegegevens die van belang konden zijn voor de opsporing en vervolging van strafbare feiten voor een bepaalde periode werden bewaard en daarmee beschikbaar waren voor opsporingsonderzoek naar ernstige misdrijven.[294]

Op 8 april 2014 heeft het Europese Hof de richtlijn met terugwerkende kracht ongeldig verklaard. Het hof was van oordeel dat met de richtlijn een te grote inbreuk is gepleegd op de bescherming van de persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens van EU-burgers. Verschillende belangenorganisaties eisten daarop in een kort geding dat de Nederlandse Wet bewaarplicht telecommunicatiegegevens ook zou worden afgeschaft. In de uitspraak van het kort geding op 11 maart 2015 gaf de rechter hen daarin gelijk.[295]

Het OM en de politie gebruikten de historische verkeersgegevens over (mobiele) telefonie en internetgebruik voor de opsporing en vervolging van zowel traditionele vormen van criminaliteit (zoals moord, gewelddadige woningovervallen, verkrachting en mensenhandel) als voor cybergerelateerde criminaliteit (zoals het hacken van systemen, het uitvoeren van DDoS-aanvallen, het downloaden van kinderporno of het online groomen van kinderen). Ook de AIVD en de MIVD maakten voor hun onderzoeken gebruik van opgeslagen telecommunicatiegegevens. In een rapport van de politie en het OM wordt het belang van de bewaarplicht voor de opsporing en vervolging bij cybergerelateerde criminaliteit toegelicht; gebruikers- en verkeersgegevens zijn dan vaak het enige aanknopingspunt voor de opsporing.[296] Daarnaast is Nederland een belangrijk internetknooppunt waar veel internationaal internetverkeer langskomt. Met een beperking of afschaffing van de bewaarplicht is het ook lastig te voldoen aan internationale verplichtingen om vragen vanuit het buitenland naar informatie over IP-adressen te beantwoorden, aldus het OM.

Het Ministerie van Veiligheid en Justitie werkt aan een wetsvoorstel dat de afgeschafte wet moet vervangen.

294 WODC (2013) De Wet bewaarplicht telecommunicatiegegevens, geraadpleegd via: https://www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bewaarplicht-telecommunicatiegegevens.aspx.

295 https://www.rechtspraak.nl/Actualiteiten/Nieuws/Pages/Wet-bewaarplicht-telecommunicatiegegevens-buiten-werking-gesteld.aspx

296 OM en Politie (2014) De bewaarplicht telecomgegevens en de opsporing - Het belang van historische telecommunicatie gegevens voor de opsporing, geraadpleegd via: http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2015/04/01/tk-bijlage-de-bewaarplicht-telecomgegevens-en-de-opsporing.html.

297 http://www.nederlandict.nl/Files/ICT/Handreiking_cyber_security_voor_de_bestuurder.pdf

298 https://www.internet.nl/about/

299 https://www.forumstandaardisatie.nl/actueel/item/titel/lancering-internetnl-tijdens-cyber-week-2015/

De belangen die de vitale sectoren beschermen blijven groot en veranderen maar weinig.



6 Belangen

Wanneer de wereld verandert, veranderen ook de gevolgen van inbreuken op cybersecurity. Berichtgeving over incidenten zorgt ervoor dat gebruikers nieuwe en bestaande diensten minder snel omarmen. Tegelijkertijd blijken ICT-systemen op nieuwe plaatsen, zoals in auto's of medische apparatuur, ook kwetsbaar te zijn voor aanvalstechnieken die gelden voor traditionele ICT-systemen. Meer toepassing van ICT gaat vaak gepaard met het afschaffen van de analoge alternatieven. Dit zorgt ervoor dat de ICT-systemen steeds belangrijker worden. Binnen deze verschuivingen blijven de belangen van de vitale sectoren groot, maar ze veranderen niet veel.

Inbreuken op cybersecurity schaden individuele, organisatorische en maatschappelijke belangen. Veranderingen in de maatschappij kunnen ertoe leiden dat de gevolgen van deze inbreuken groter of kleiner worden. Dit hoofdstuk beschrijft relevante ontwikkelingen in die belangen.

Verminderd vertrouwen in digitale diensten remt bedrijvigheid

Veel mensen beginnen digitale diensten merkbaar minder te vertrouwen door berichtgeving over de betrouwbaarheid van ICT-systemen. Berichten over datalekken, uitval van ICT en de Snowden-onthullingen zorgen ervoor dat mensen terughoudend worden met het gebruik van die systemen.

Zo gaf in het afgelopen jaar een kwart van de Nederlanders aan minder te internetbankieren, online te kopen en apps op hun telefoon te gebruiken.[300] Wanneer mensen minder gebruikmaken van digitale diensten, kan dit een rem vormen op de economische groei. Ook andere diensten, zoals sociale media, vonden minder aftrek. Het effect van verminderd vertrouwen op het gebruik was daar wel kleiner. Redenen voor deze terughoudendheid waren meestal onvoldoende privacywaarborgen, onvoldoende beveiliging en onvoldoende beschikbaarheid van de dienst.

Zorgen over privacy zijn voor gebruikers een belangrijke motivatie om zichzelf beter te beschermen. Aanbieders van mobieleberichtendiensten sprongen hierop in door het aanbieden van zogeheten 'end-to-end'-encryptie. Het gebruik van deze encryptie zorgt ervoor dat de aanbieder van de dienst de inhoud van de berichten wniet kan lezen. Een bekend voorbeeld is de end-to-end-encryptie in de Android-versie van berichtendienst WhatsApp.[301]

Nieuwe toepassingsgebieden leveren kwetsbaarheden en debat op

ICT wordt op nieuwe manieren toegepast. Daardoor kan een inbreuk op de beveiliging nieuwe gevolgen hebben. Bevat een koelkast bijvoorbeeld software en is deze met een netwerk verbonden, dan kan een malwarebesmetting gevolgen hebben voor de voedselveiligheid. De aanvaller kan dan de temperatuurinstelling van de koelkast op afstand verhogen, waardoor het eten bederft. Deze risico's kunnen ook ontstaan als de gebruikte software bugs bevat, een licentie verloopt of een netwerkdienst

300 http://publications.tno.nl/publication/34611864/kSscvS/TNO-2014-R11119.pdf
301 Zie ook: http://www.nrcq.nl/2014/11/18/whatsapp-gaat-versleuteling-aanbieden-in-een-volgende-update.

niet meer bereikbaar is. Beveiliging heeft vaak geen prioriteit bij het ontwikkelen van dit soort nieuwe toepassingen.

Gedigitaliseerde mobiliteit vergt gescheiden netwerken

Auto's, vliegtuigen en andere vervoermiddelen worden voorzien van meer ICT-mogelijkheden. Dat vraagt om aandacht voor de beveiliging. Het is immers niet de bedoeling dat een beveiligingsprobleem in een entertainmentsysteem aan boord gevolgen heeft voor de besturing van het voertuig. Een gebrek aan beveiliging kan dan zelfs fatale gevolgen hebben.

Ontwikkelingen bij het beveiligen van deze 'gedigitaliseerde mobiliteit' richten zich vooral op het scheiden van netwerken. Zowel bij auto's als bij vliegtuigen was er aandacht voor de risico's die ontstaan als interne ICT-systemen met een verschillend beveiligingsniveau gekoppeld worden.
In de luchtvaart mogen passagiers steeds vaker eigen apparaten gebruiken tijdens de vlucht. Verschillende maatschappijen bieden hun passagiers al draadloze internetfaciliteiten. Vanzelfsprekend moeten deze netwerken gescheiden blijven van de besturing van het vliegtuig. Een onderzoeker die twitterde over een vermeende koppeling tussen deze systemen, werd door United Airlines van zijn vlucht geweerd.[302] Het Amerikaanse Government Accountability Office achtte een dergelijke aanval erg onwaarschijnlijk.[303] Dit zal echter sterk afhangen van de getroffen maatregelen.

Nieuwe auto's bevatten allerlei ICT-systemen, variërend van een intern entertainmentsysteem tot mogelijkheden voor de fabrikant om de auto op afstand te openen. Deze systemen hebben vaak nauwelijks iets te maken met de besturing van de auto. Is er echter geen scheiding aangebracht tussen deze systemen en de systemen die de besturing regelen, dan kan een aanvaller een kwetsbaarheid in een dergelijk ICT-systeem gebruiken om de besturing van de auto te beïnvloeden. De aanvaller kan dan bijvoorbeeld een ongeluk veroorzaken. Al in 2011 wisten onderzoekers zulke kwetsbaarheden uit te buiten en de besturing van een auto op afstand te beïnvloeden.[304]

De ontwikkeling van zelfsturende auto's gaat in de toekomst ongetwijfeld meer beveilingsvraagstukken met zich meebrengen. In een dergelijke auto regelt een ICT-systeem de besturing. Het valt te verwachten dat dit in de komende jaren een belangrijk punt van discussie zal zijn.

Medische apparaten zijn inmiddels ook computers, wat vergelijkbare dreigingen oplevert

ICT-systemen in de medische wereld zorgen ervoor dat alledaagse kwetsbaarheden gevolgen kunnen hebben voor de gezondheid van patiënten. Medische apparaten kunnen steeds vaker op afstand worden beheerd, bijvoorbeeld via wifi of bluetooth. Weet een aanvaller dit beheer over te nemen, dan kan hij de betrokken patiënten kwaad doen. Gaat het om een apparaat dat vitale lichaamsfuncties in stand houdt, dan kan dat fatale gevolgen hebben.

In een onderzoek van Deloitte naar de beveiliging van medische apparatuur in Nederlandse ziekenhuizen bleek een meerderheid van de geïnterviewde instellingen ervaring te hebben met malwarebesmettingen op hun medische apparatuur.[305] Dit is een indicatie voor de complexiteit en de kwetsbaarheid van zulke apparaten. Omdat het volledige computers zijn geworden, worden ze geconfronteerd met dezelfde risico's als traditionele systemen.

Analoge alternatieven verdwijnen

Wanneer ICT-systemen voor de ondersteuning van maatschappelijke processen niet beschikbaar zijn, is er in een groeiend aantal gevallen geen analoog alternatief meer. De beschikbaarheid van deze ICT-systemen wordt daarmee belangrijker: uitval is geen optie. Tegelijkertijd is de onderliggende technologie complexer dan bij analoge systemen. Ook zijn deze systemen gemakkelijker aan te vallen als ze via het internet bereikbaar zijn.

Wanneer een ICT-systeem dat een maatschappelijk proces ondersteunt uitvalt, is de maatschappij aangewezen op analoge alternatieven. Zijn er geen analoge alternatieven beschikbaar, dan heeft een dergelijke uitval ernstige gevolgen. Valt het internetbankieren uit, dan zijn de gevolgen ernstiger als klanten niet ook bij een bankkantoor terecht kunnen.

Tegelijkertijd zijn ICT-systemen complexer dan hun analoge alternatieven. Dat maakt ze sneller vatbaar voor uitval. Hun infrastructuur is geografisch verspreid, vaak zelfs wereldwijd. Veel organisaties weten niet welke ICT-systemen cruciaal voor hen zijn. Ook maakt de complexiteit van hard- en software het onmogelijk om het gedrag van een systeem in alle gevallen te voorspellen.

Voorbeeld: de overheid streeft naar digitaal contact met burgers

De overheid streeft ernaar om burgers en bedrijven steeds meer zaken digitaal te laten regelen. Dat staat in het visieplan Digitale overheid 2017.[306]

Overheden willen sommige diensten alleen nog digitaal verlenen. Een aantal gemeenten heeft in de afgelopen jaren besloten officiële bekendmakingen alleen nog maar digitaal te publiceren.[307]
De Belastingdienst stelt digitaal aangifte doen voor bepaalde

302 https://nakedsecurity.sophos.com/2015/04/20/security-researcher-barred-from-united-airlines-flight-after-hack-tweet/
303 http://www.gao.gov/products/GAO-15-370
304 http://www.nytimes.com/2011/03/10/business/10hack.html
305 http://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/cyber-security-medische-apparatuur-beeld.html
306 Zie ook: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017.html.
307 Bijvoorbeeld: http://www.nrc.nl/handelsblad/van/2015/januari/02/gemeente-bekendmakingen-alleen-nog-maar-digitaal-1446984.

belastingen verplicht voor ondernemers.[308] De gemeente Tilburg liet in juli 2014 weten dat bijstandsuitkeringen alleen nog maar digitaal aangevraagd kunnen worden.[309] Een onderzoek in Amsterdam liet echter zien dat burgers voor lang niet alle zaken behoefte hebben aan digitaal contact met de overheid.[310]

Voorbeeld: het betalingsverkeer kent steeds minder analoge alternatieven

Het betalingsverkeer verschoof de afgelopen jaren van contanten en transacties op papier naar digitale systemen. Voor consumenten is het nog maar beperkt mogelijk om te bankieren zonder te beschikken over een internetverbinding. Regelmatig moeten zij daarvoor aanvullende kosten maken.[311]

Ook betalen met contant geld wordt op minder plaatsen mogelijk. Bij veel automaten, maar ook in sommige winkels, kan niet langer met contant geld worden afgerekend. Is het pinverkeer niet beschikbaar, dan is het in deze winkels nog wel mogelijk om te betalen met een zogeheten Eenmalige Machtiging Pinnen.[312] Bij automaten bestaat die mogelijkheid echter niet.

Hoewel bankieren met analoge middelen nog maar beperkt mogelijk is, bieden banken en andere aanbieders wel steeds vaker digitale alternatieven. De meeste banken bieden naast het internetbankieren bijvoorbeeld ook een eigen app. Is een van beide kanalen niet toegankelijk, dan is het andere soms nog wel beschikbaar.[313] Ook de populariteit van alternatieve betaaldiensten als PayPal komt de beschikbaarheid van het betalingsverkeer ten goede.

Belangen van vitale sectoren zijn groot maar stabiel

De belangen die de vitale sectoren beschermen blijven groot en veranderen maar weinig. Dat blijkt uit gesprekken met vertegenwoordigers van organisaties in deze sectoren. Hoewel het beveiligen van informatie en systemen telkens nieuwe uitdagingen creëert, zijn de achterliggende redenen voor het beveiligen nauwelijks veranderd. Hieronder worden drie voorbeelden uit de sectoren kort toegelicht.

De energiesector is verantwoordelijk voor een betrouwbare en ongestoorde energievoorziening. Enkele ontwikkelingen veranderen de aard van de dreiging en te treffen maatregelen. Een voorbeeld is de invoering van de slimme meter. Uiteindelijk dient ook deze ontwikkeling echter hetzelfde doel.

Rampen- en crisiscommunicatie maakt gebruik van IP-technologie

Ook crisiscommunicatiesystemen worden gedigitaliseerd. Dit zorgt voor betere beheermogelijkheden en functionaliteit. Tegelijkertijd is de beschikbaarheid van de gebruikte technologie een aandachtspunt in de omzetting.

De Noodcommunicatievoorziening (NCV) maakt gebruik van IP-technologie voor de communicatie tussen aangesloten partijen.[314] De NCV is het netwerk voor communicatie tussen vitale organisaties in geval van een crisis. De NCV voorziet in communicatie via vaste en mobiele telefonie en dataverbindingen. In 2010 heeft de NCV diens voorganger, het Nationaal Noodnet, opgevolgd.[315] De NCV is zo ontworpen dat hij nog beschikbaar is als het gewone telefoonverkeer uitvalt tijdens een ramp.

De Nederlandse goederentransportsector dient het economische belang van Nederland als centrale partij in distributie van goederen. Verstoringen kunnen dat belang schaden, omdat het transport dan via andere landen plaats moet vinden. Langdurige verstoringen raken de samenleving ook op een dieper niveau: de voedselvoorziening is in belangrijke mate afhankelijk van deze sector.

De telecomsector vervult een faciliterende rol voor andere vitale sectoren. Het netwerk voor elektronische communicatie wordt bijvoorbeeld gebruikt voor de geautomatiseerde aansturing van procescontrolesystemen. Systemen als 112 en NL-Alert zijn voor de communicatie met burgers afhankelijk van de goede werking van het netwerk voor elektronische communicatie.

Conclusie en vooruitblik

De betrouwbaarheid van software wordt belangrijker nu ICT-systemen op meer plaatsen worden toegepast. Mobiliteit en medische apparatuur vormen hiervan illustraties. De impact van een inbreuk kan bij deze toepassingen veel groter zijn, omdat de systemen directe invloed hebben op de fysieke omgeving van mensen. Deze inbreuken zijn zeker niet denkbeeldig, omdat de

308 http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/aangifte_betalen_en_toezicht/aangifte_doen/
309 http://www.tilburg.nl/actueel/nieuws/item/nieuwe-werkwijze-aanvraag-uitkering/
310 https://www.utwente.nl/nieuwsevents/!/2015/1/346014/digitaal-vaardige-burgers-willen-niet-altijd-digitaal
311 http://www.consumentenbond.nl/betaalrekening/Extra/bankeren-zonder-internet/
312 http://www.betaalvereniging.nl/wp-uploads/2014/05/Betaalwijzer_mei_2014.pdf
313 Bijvoorbeeld: https://tweakers.net/nieuws/102469/internetbankieren-ing-kampt-met-storing.html.
314 http://www.telecompaper.com/nieuws/kpn-levert-ipnetwerk-voor-noodcommunicatie-overheden--703707
315 Zie ook: http://www.rijksoverheid.nl/nieuws/2009/11/18/nieuw-noodcommunicatienetwerk-voor-bestuurlijk-nederland-en-vitale-organisaties-bij-ramp-of-crisis.html.

digitale beveiliging lang niet altijd prioriteit heeft. Het valt niet te verwachten dat deze situatie zal veranderen zonder externe prikkels, zoals een incident of regulering.

Wie verantwoordelijk is voor een maatschappelijk proces, bewaakt ook de beschikbaarheid van de onderliggende ICT-systemen. Op deze manier is er oog voor de gevolgen die een uitval van ICT-systemen kan hebben op de maatschappij.

De belangen van de vitale sectoren blijven ook de komende jaren gelijk. De organisaties in deze sectoren zijn door hun ervaring steeds beter in staat om voor deze belangen in te staan.

Bijlagen

Bijlage 1 NCSC-statistieken

Deze bijlage biedt een overzicht van de responsible disclosures, beveiligingsadviezen en incidenten die door het NCSC zijn afgehandeld.

Het NCSC faciliteert het doen van responsible-disclosuremeldingen voor zowel zijn eigen infrastructuur als die van de Rijksoverheid en enkele private partijen. Het brengt beveiligingsadviezen uit aan zijn deelnemers en handelt cybersecurityincidenten af. Hierover zijn voor deze rapportageperiode statistieken berekend die hieronder worden gepresenteerd. Door deze statistieken te vergelijken met eerdere rapportageperiodes kunnen trends en overige ontwikkelingen worden geïdentificeerd.

Responsible disclosure

In 2013 heeft het NCSC een leidraad responsible disclosure[316] gepubliceerd en tegelijkertijd een responsible-disclosurebeleid[317] voor zijn eigen website uitgebracht. In 2015 heeft het NCSC samen met zijn partners een 'best practice guide'[318] uitgebracht om ervaringen op dit gebied te delen en daarmee andere organisaties te helpen met het implementeren of verbeteren van hun eigen responsible-disclosurebeleid. Met deze publicaties heeft het NCSC bijgedragen aan het op een verantwoorde wijze melden en afhandelen van kwetsbaarheden in informatiesystemen en (software) producten. Mede door deze publicaties is het NCSC zichtbaarder geweest en hebben meer melders het weten te vinden. Dit heeft vervolgens geleid tot aanzienlijk meer meldingen in deze periode. Ook hebben sommige melders (20 procent van het totaal) in deze periode meerdere meldingen gedaan. Dit suggereert dat hun ervaringen positief waren en de interactie met het NCSC zinvol was.

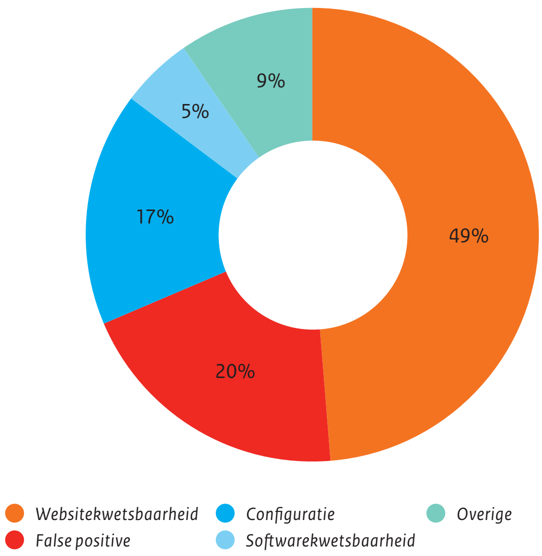
In de rapportageperiode heeft het NCSC ruim 150 meldingen ontvangen. Dit waren zowel meldingen voor eigen systemen als voor overige overheidssystemen en systemen van private partijen. In sommige gevallen was er sprake van een dubbele melding, bijvoorbeeld als twee of meer onderzoekers dezelfde kwetsbaarheid gemeld hadden. Hierdoor is het totale aantal meldingen niet representatief voor het totale aantal kwetsbaarheden. In 20 procent van alle meldingen was er bij nader onderzoek geen sprake van een kwetsbaarheid. Deze gevallen werden geclassificeerd als *false positive*.

Figuur 10 toont de verschillende typen meldingen, inclusief de eerdergenoemde false positives. Iets minder dan de helft (49 procent) van alle meldingen had te maken met een kwetsbaarheid in een website, een webapplicatie of infrastructuur waarop webapplicaties draaien. Voorbeelden van zulke meldingen zijn Cross-Site Scripting (XSS) of SQL-injectie. Ongeveer een zesde (17 procent) van alle meldingen had te maken met een fout in de configuratie van een softwareproduct, zoals een webserver. Voorbeelden van zulke meldingen zijn het ondersteunen van een verouderde TLS-versie of het gebrek aan bepaalde http-headers. Slechts 5 procent van alle meldingen had te maken met kwetsbaarheden in software (exclusief webservers of -applicaties). Een voorbeeld hiervan is een kwetsbaarheid in een applicatie voor smartphones. Tot slot had 9 procent van alle melding te maken met overige kwetsbaarheden die niet tot een van de genoemde types horen. Voorbeelden van zulke meldingen zijn een kwetsbaarheid in een hardwareproduct van een private partij of de mogelijkheid om gevoelige gegevens te achterhalen door gebruik te maken van een commerciële dienst.

Vergeleken met de vorige rapportageperiode zijn er in de afgelopen periode ongeveer 50 procent meer meldingen gedaan. In totaal waren er nu ongeveer evenveel meldingen over websitekwetsbaarheden als tijdens de vorige rapportageperiode. Hun aandeel in het totaal is echter met 25 procentpunt afgenomen. In de vorige periode ging het om 76 procent van de 95 meldingen, ten opzichte van 51 procent van 156 meldingen tijdens deze periode. Dit heeft waarschijnlijk te maken met een substantiële stijging in false positives en overige meldingen.

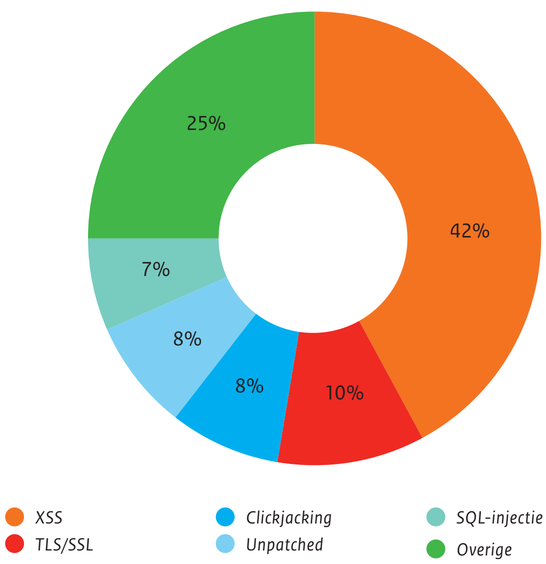
316 https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html
317 https://www.ncsc.nl/security
318 https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-presenteert-best-practice-guide-responsible-disclosure-in-aanloop-naar-de-global-conference-on-cyberspace.html

Figuur 10 **Typen responsible-disclosuremeldingen**



Aangezien het overgrote deel van de meldingen in het kader van responsible disclosure kwetsbaarheden in websites betreft, wordt dit type kwetsbaarheid nader geanalyseerd in figuur 11. Deze figuur laat zien dat veel websitekwetsbaarheden (42 procent) te maken hebben met XSS. In de vorige periode vormde XSS ongeveer 50 procent van alle websitekwetsbaarheden. Deze afname heeft waarschijnlijk te maken met een substantiële stijging in het aantal overige websitekwetsbaarheden. Voorbeelden van zulke kwetsbaarheden zijn kwetsbare authenticatiemechanismen of gevoelige informatie die te vinden is via openbare zoekmachines. Onder ‘overige’ meldingen vallen bijvoorbeeld intranetpagina’s die via het internet te bereiken waren en kwetsbare authenticatiemechanismen.

Figuur 11 **Gemelde websitekwetsbaarheden**



Beveiligingsadviezen

Het NCSC publiceert beveiligingsadviezen (oftewel advisories) naar aanleiding van softwarekwetsbaarheden of geconstateerde dreigingen. In een beveiligingsadvies wordt beschreven wat er aan de hand is, welke systemen getroffen zouden kunnen zijn en wat er moet gebeuren om te voorkomen dat een organisatie slachtoffer wordt. Figuur 12 toont het aantal advisories dat het NCSC per kwartaal heeft gepubliceerd vanaf het tweede kwartaal van 2003 tot en met het eerste kwartaal van 2015. Hierbij wordt er onderscheid gemaakt tussen nieuwe advisories (met versienummer 1.00) en updates op bestaande advisories.

De beveiligingsadviezen van het NCSC worden ingeschaald op twee elementen. Ten eerste stelt men vast wat de kans is dat de kwetsbaarheid misbruikt wordt. Ten tweede bepaalt men de schade die optreedt wanneer de kwetsbaarheid misbruikt wordt. De inschaling kent dus twee criteria: kans en schade. Voor beide criteria wordt, op basis van meerdere aspecten, een niveau geschat: hoog (H), gemiddeld (M) of laag (L). Bijvoorbeeld: als er een hoge kans is dat een bepaalde kwetsbaarheid misbruikt wordt, maar de verwachte schade van misbruik is laag, dan krijgt het bijbehorende beveiligingsadvies een H/L-inschaling. Figuur 13 toont de verhoudingen tussen deze niveaus van alle gepubliceerde adviezen in de rapportageperiode.

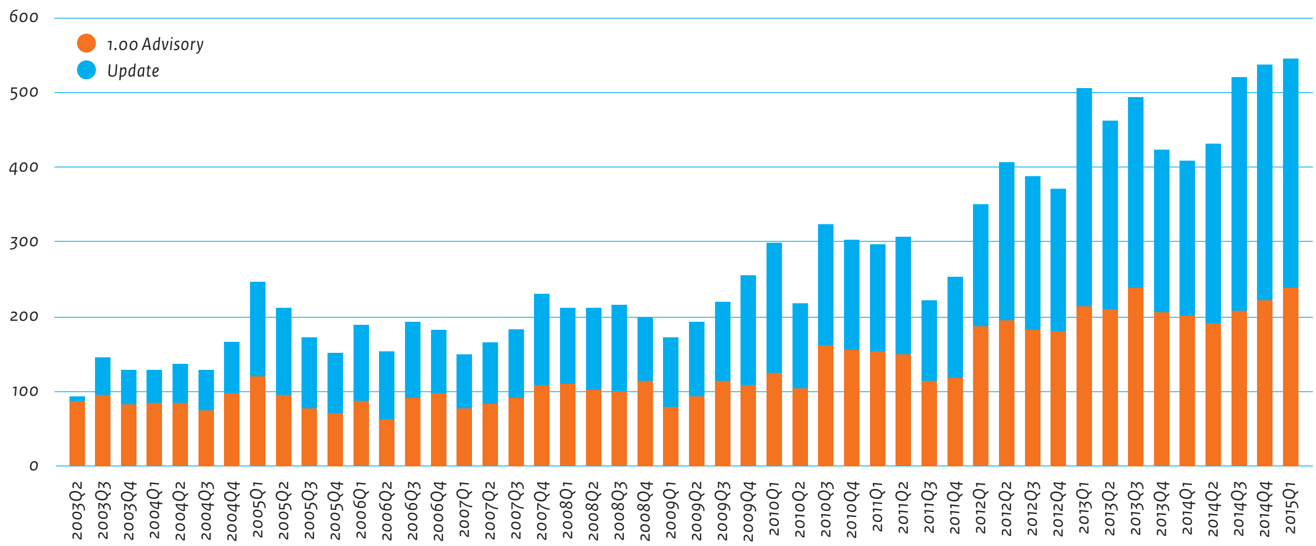
Schade van kwetsbaarheden in software

Bij ieder beveiligingsadvies hoort een omschrijving van de mogelijke schade die een kwaadwillende zou kunnen verrichten als het advies niet gevolgd wordt. Om een overzicht te krijgen van deze schade worden adviezen gecategoriseerd op basis van een standaardlijst van schadeomschrijvingen. Voor de rapportageperiode

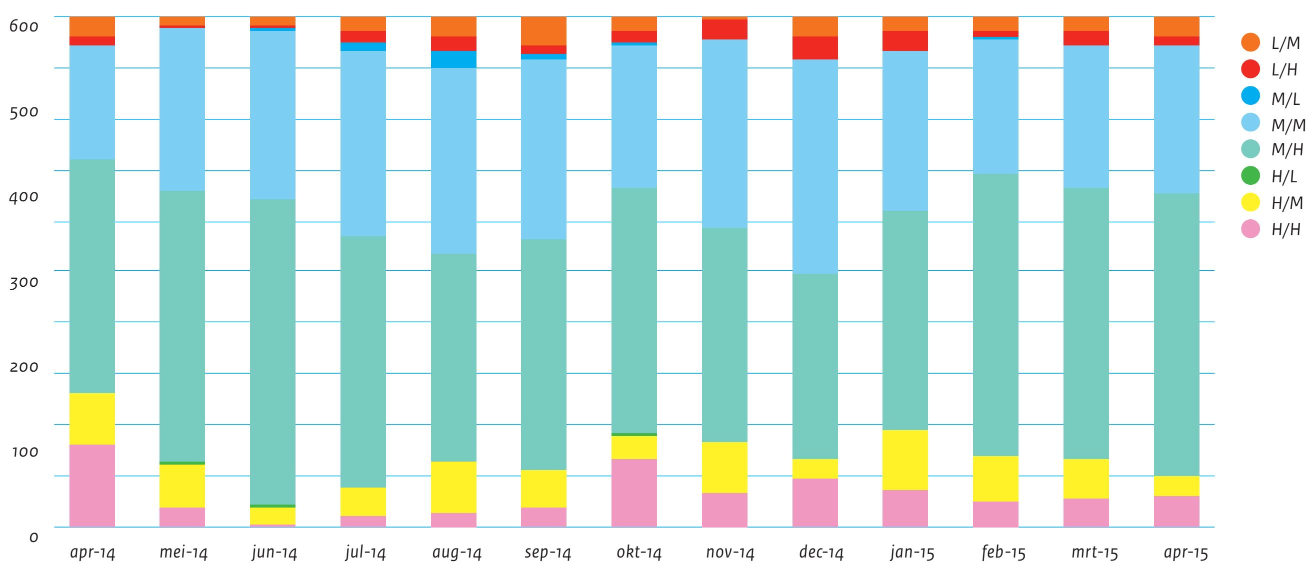
Tabel 4 **Percentage beveiligingsadviezen per schadeomschrijving**

Schadeomschrijving	%
Denial-of-Service (DoS)	51%
Remote code execution (Gebruikersrechten)	29%
Toegang tot gevoelige gegevens	26%
Omzeilen van beveiligingsmaatregel	19%
Verhoogde gebruikersrechten	14%
Toegang tot systeemgegevens	9%
Cross-Site Scripting (XSS)	6%
Manipulatie van gegevens	5%
Omzeilen van authenticatie	4%
Remote code execution (Administrator/Rootrechten)	4%
Spoofing	2%
Cross-Site Request Forgery (XSRF)	1%
SQL-Injectie	1%

Figuur 12 **Aantal advisories per kwartaal (2003Q2 - 2015Q1)**



Figuur 13 **Inschaling advisories in de rapportageperiode**



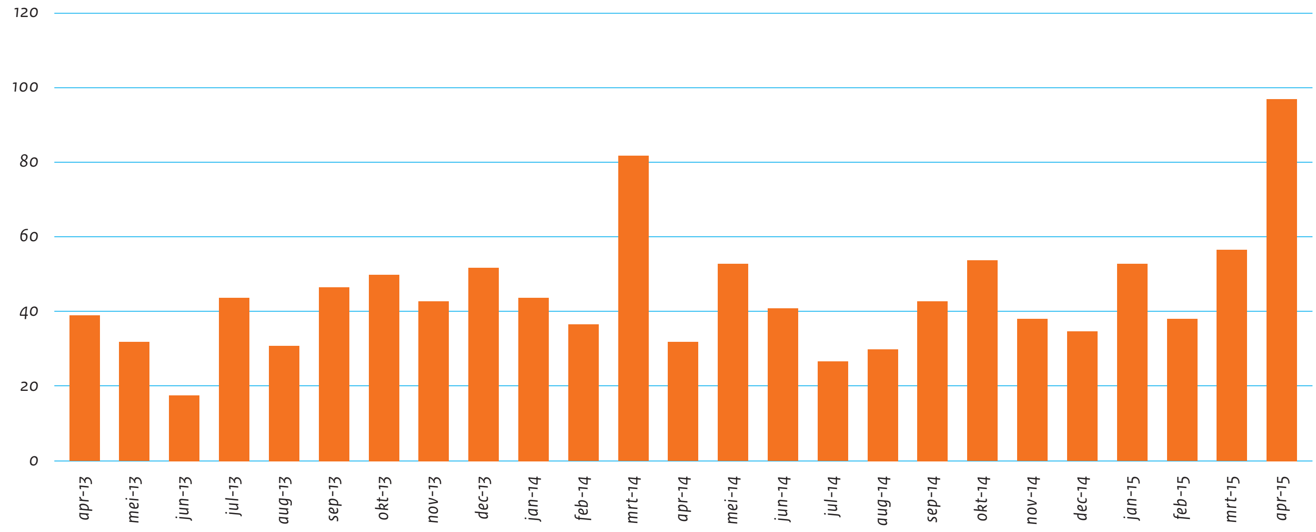
wordt het percentage adviezen per schadeomschrijving in Tabel 4 getoond. Hierin is duidelijk te zien dat het grootste aantal beveiligingsadviezen (51 procent) te maken had met Denial-of-Service (DoS). Hierna volgen het uitvoeren van willekeurige code met gebruikersrechten (29 procent), toegang tot gevoelige gegevens (26 procent) en het omzeilen van een beveiligingsmaatregel (19 procent). Regelmatig zijn bij een advies meerdere schadeomschrijvingen van toepassing.

Het NCSC ondersteunt overheden en organisaties in vitale sectoren bij het afhandelen van incidenten op het gebied van ICT-veiligheid. In die rol worden bij het NCSC incidenten en kwetsbaarheden gemeld. Ook identificeert het NCSC deze zelf, bijvoorbeeld op basis van diverse detectiemechanismen. Daarnaast bemiddelt het NCSC op verzoek van (inter)nationale partijen met Nederlandse internet-serviceproviders om te ondersteunen bij het bestrijden van ICT-veiligheidsincidenten die hun oorsprong vinden in Nederland (bijvoorbeeld vanaf een malafide webserver of vanaf geïnfecteerde pc's in Nederland).

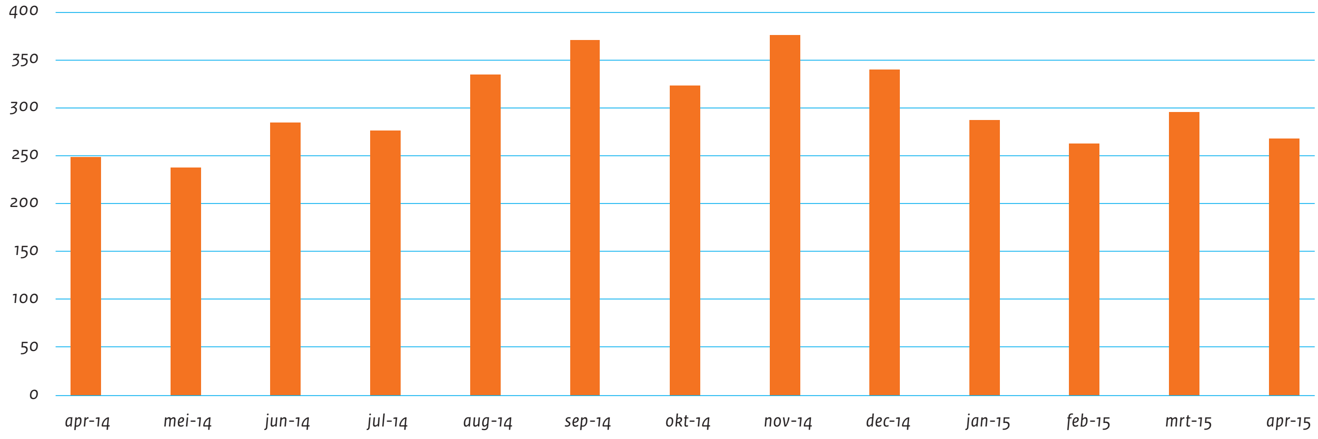
Aantallen afgehandelde incidenten

Het aantal incidentmeldingen dat het NCSC in de rapportageperiode heeft afgehandeld, wordt anders berekend en gepresenteerd dan in vorige versies van het CSBN. De reden hiervoor is als volgt. In het laatste kwartaal van 2013 heeft het NCSC een deel van haar incidentmeldingen geautomatiseerd. Dit heeft geleid tot een sterke

Figuur 14 **Afgehandelde incidenten (exclusief geautomatiseerde controles)**



Figuur 15 **Geautomatiseerde controles**



stijging (ongeveer 400 procent) in het aantal afgehandelde incidenten terwijl de actuele dreiging weinig veranderd is. In het vorige CSBN werden deze geautomatiseerde controles opgeteld bij alle andere incidenten. In dit CSBN worden deze los getoond.

Figuur 14 toont het aantal afgehandelde incidenten per maand voor de periode april 2013 tot en met april 2015. Behalve enkele afwijkingen in maart 2014 en april 2015 is het aantal incidenten relatief stabiel gebleven. Dit is ook te zien in de absolute aantallen. In de vorige rapportageperiode waren er in totaal 519 incidenten gemeld. In deze rapportageperiode zijn er 598 incidenten gemeld (exclusief geautomatiseerde controles). Het verschil kan deels verklaard worden door het feit dat de huidige periode iets langer is dan de vorige: 13 maanden in plaats van 12.

Figuur 15 toont de resultaten van geautomatiseerde controles voor de rapportageperiode. Hieruit blijkt dat er gemiddeld 300 incidentmeldingen per maand zijn op basis van deze automatisering. Een melding kan meerdere geïnfecteerde systemen binnen een organisatie betreffen.

Figuur 16 toont de afgehandelde incidenten (exclusief geautomatiseerde controles) uitgesplitst naar hulpmiddel. In deze context is een hulpmiddel het type aanval, dat geleid heeft tot het incident. Voor een groot deel is het begrip ‘hulpmiddel’ niet van toepassing, bijvoorbeeld bij een responsible-disclosuremelding over verouderde software. De overgebleven incidenten betreffen vooral phishing, ransom- en cryptoware en information leakage. Is phishing het hulpmiddel, dan betreft het incident vaak een notice-and-takedownverzoek (NTD). De totalen van deze uitsplitsing kunnen afwijken van de hierboven vermelde totalen, omdat bij sommige incidenten meerdere hulpmiddelen gebruikt zijn en deze dus meerdere malen geteld zijn.

Cybersecurityincidenten geregistreerd bij het NCSC

Onder incident verstaat het NCSC hier 'een ICT-gerelateerd beveiligingsvoorval dat is gemeld of ontdekt waarbij zich een acuut gevaar voor of schade aan ICT-systemen of elektronische informatie voordeed, betrekking hebbend op een of meer specifieke organisaties, waarop NCSC reactief heeft opgetreden richting deze organisaties.' Volledig geautomatiseerde meldingen vallen buiten deze definitie. Deze afbakening geeft aan dat een incident niet altijd al tot schade heeft geleid, maar ook een gevaar kan zijn zonder dat al schade is veroorzaakt. Incidenten vallen in drie soorten uiteen:

Aanval: er heeft daadwerkelijk een (poging tot een) aanval plaatsgevonden met zo mogelijk een inbreuk op de beveiliging tot gevolg. Hierbij gaat het bijvoorbeeld om hacks, malware-infecties of DDoS-aanvallen.

Dreiging: er bestaat een kwaadaardige intentie bij een actor om een aanval uit te voeren, maar deze is nog niet uitgevoerd.
Kwetsbaarheid: een ICT-omgeving is kwetsbaar, als gevolg van bijvoorbeeld een fout in software, hardware of systeemconfiguratie. Bij een kwetsbaarheid is (nog) geen sprake van een dreiging of aanval, maar er is wel gelegenheid tot misbruik.

Figuur 17 toont een uitsplitsing van de afgehandelde incidenten per type. Hieruit blijkt dat responsible-disclosuremeldingen een substantieel aandeel vormen (26 procent). Daarna zijn NTD-meldingen de meest voorkomende incidenten. De meeste NTD-verzoeken zijn verzoeken van Nederlandse financiële instellingen om hulp bij het bestrijden van phishingaanvallen. Deze aanvallen richten zich op deze instellingen. De oorsprong bevindt zich veelal in het buitenland.

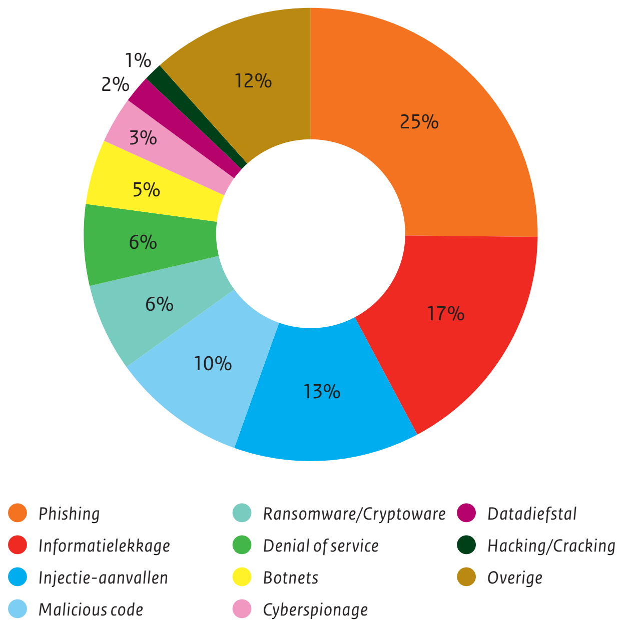
Verdeling incidenten tussen overheid en vitale sectoren

Het NCSC ondersteunt zowel de Rijksoverheid als de vitale sectoren bij beveiligingsincidenten. Daarnaast treedt het NCSC op als contactpunt voor internationale hulpverzoeken met betrekking tot informatiebeveiliging.

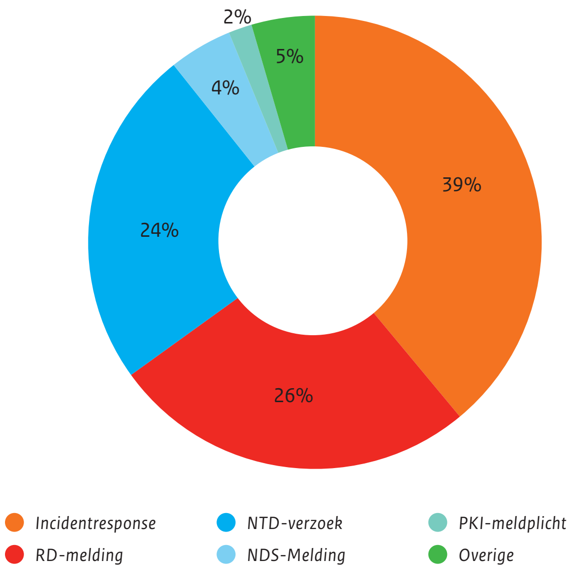
In figuur 18 is te zien wat de opbouw is van het aantal afgehandelde incidenten, uitgesplitst naar type betrokken organisatie. De verdeling tussen private en publieke organisaties varieert niet veel gedurende de rapportageperiode. In totaal was bij 50 procent van de incidenten een publieke organisatie betrokken. Bij 40 procent ging het om een private organisatie. De resterende 10 procent betrof een internationaal hulpverzoek. Het aantal internationale hulpverzoeken varieert sterker gedurende de rapportageperiode, van 3 procent in april 2014 tot 16 procent in april 2015.

Figuur 19, figuur 20 en figuur 21 tonen de opbouw van de incidenten waarbij verschillende typen organisaties bij betrokken waren. Het type incidenten waarbij overheidsorganisaties en private partijen

Figuur 16 Afgehandelde incidenten per hulpmiddel



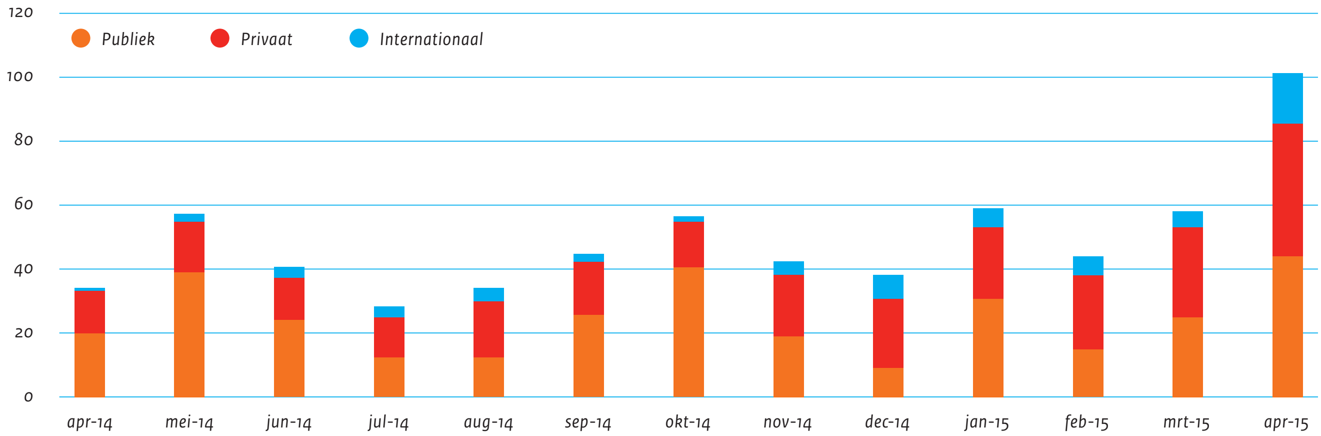
Figuur 17 Afgehandelde incidenten per type



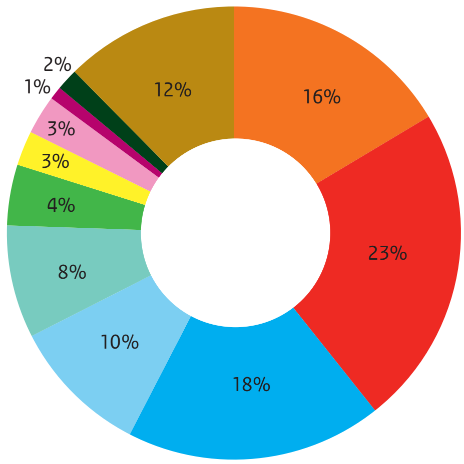
betrokken zijn, loopt niet sterk uiteen. Wel is duidelijk dat private partijen relatief vaak om ondersteuning vragen bij phishingincidenten. Dit omvat bijvoorbeeld verzoeken om ondersteuning bij het onbeschikbaar maken van een phishingwebsite voor een bank. Overheden zijn vaker betrokken bij incidenten rond informatielekken en injectieaanvallen. Dit betreft bijvoorbeeld RD-meldingen van kwetsbaarheden in websites van overheidsorganisaties.

De internationale hulpverzoeken kennen wel een duidelijk andere opbouw. De helft van de verzoeken betreft phishing, waarbij het vaak gaat om verzoeken om phishingwebsites onbeschikbaar te maken.

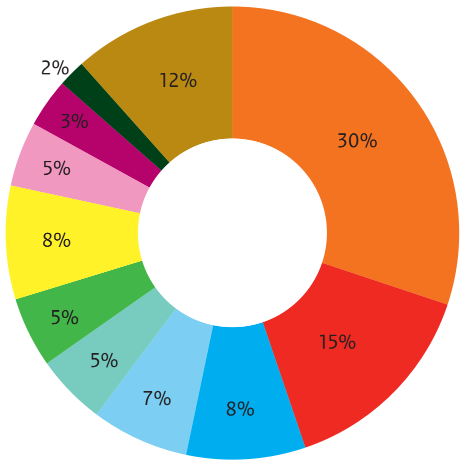
Figuur 18 Afgehandelde incidenten per maand per type organisatie



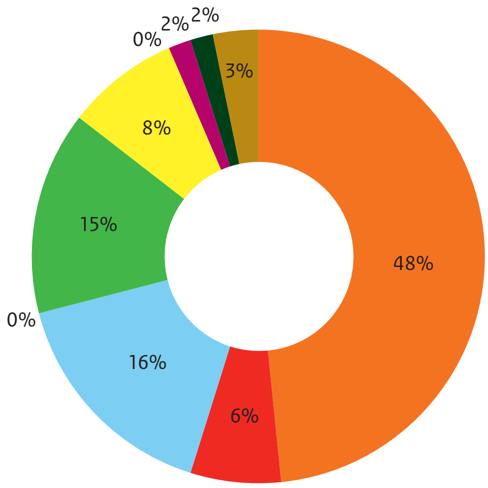
Figuur 19 Type incidenten waarbij een overheidspartij betrokken was

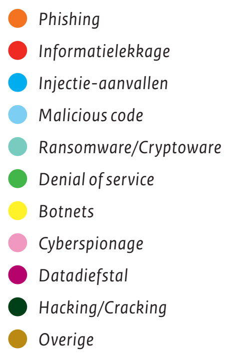


Figuur 20 Type incidenten waarbij een private partij betrokken was



Figuur 21 Type incidenten waarvoor het NCSC een internationaal hulpverzoek ontving





Bijlage 2 Cybersecurity in de vitale sectoren

Bij het opstellen van het Cybersecuritybeeld Nederland zijn er gesprekken gevoerd met vertegenwoordigers van de Nederlandse vitale sectoren. Deze gesprekken hebben geholpen de analyses in dit CSBN te richten en inzichten te onderbouwen. Deze bijlage geeft het beeld weer dat deze vertegenwoordigers schetsten gedurende de gesprekken.

Sector	Manifestaties	Dreigingen: actoren	Dreigingen: middelen
Drinkwatervoorziening	Er zijn geen grote incidenten geweest.	De sector ervaart geen grote dreiging van bepaalde categorieën actoren.	Malware en phishing op de kantoorautomatisering; malware op procesautomatisering.
Energie	Er zijn geen grote incidenten geweest.	De dreigingen die specifiek zijn voor deze sector worden gevormd door statelijke actoren, hacktivisten en interne actoren. Daarnaast kunnen de grote belangen een interessant doelwit zijn voor afpersing door criminelen.	Geavanceerde middelen zijn toegankelijker voor hacktivisten. DDoS-as-a-service met behulp van booterservices is hiervan een voorbeeld. Daarnaast vindt veel (spear)phishing plaats.
Financiële instellingen	Het aantal incidenten met identiteits-fraude blijft hoog. Hierbij richten daders zich niet alleen op personen, maar ook op bedrijven. DDoS-aanvallen zijn er in de rapportage-periode wel geweest, maar niet groter dan in 2013.	Criminelen vormen nog altijd de grootste dreiging voor de belangen die de sector vertegenwoordigt.	Criminelen worden steeds professio-neler. Kwaliteit van de Phishing-e-mails en (soms) gerichtheid van phishing valt daarbij op. Sommige aanvallen lijken pas te worden uitgevoerd na maanden 'oogsten' van informatie. De aard van DDoS-aanvallen in de rest van de wereld wordt steeds gevarieerder. Deze trend is nog niet zichtbaar bij Nederlandse financiële instellingen gedurende de rapporta-geperiode.
Managed Service Providers	De stroomstoring in Diemen heeft geleid tot communicatiestoringen in zowel data- als spraaknetwerken (met name GSM). Hierdoor werd de dienstverlening van serviceproviders in heel Noord-Holland en delen van Flevoland verstoord. Dit illustreert de afhankelijk van energielevering van de sector.	De grootste dreigingen voor deze sector gaan uit van statelijke actoren en criminelen. Het beeld bestaat dat de capaciteiten van terroristen groeien, wat hen een relevantere dreiging kan maken.	Eindgebruikers van klantorganisaties kampen regelmatig met cryptoware-aanvallen. Er is veel phishing en andere social engineering waargeno-men. Daarnaast maakt de sector zich zorgen over het achterhouden van zero-daykwetsbaarheden door overheden.

Weerbaarheid: kwetsbaarheden	Weerbaarheid: maatregelen	Belangen
Veel innovatieve diensten (niet zijnde primaire processen, bijvoorbeeld meldingen van storingen) maken gebruik van clouddiensten.	Bewustwording personeel; meer sector-interne samenwerking en samenwerking met NCSC; meer zonering en monitoring in netwerken voor beveiliging van SCADA-systemen.	De drinkwatervoorziening is van groot belang voor de volksgezondheid en voor het functioneren van de samenleving. Uitval leidt tot sociaal-maatschappelijke ontwrichting.
Vergaande scheiding van netwerken maakt de feitelijke energielevering minder kwetsbaar. De systemen daar omheen die handel mogelijk maken zijn wel verbonden met internet. Er is soms sprake van een monocultuur omdat sommige ICT-leveranciers aan (bijna) alle energiebedrijven leveren. Remote access tot apparatuur kent voordelen voor beschikbaarheid, maar creëert ook aangrijpingspunten voor aanvallen.	Incidentrespons krijgt meer aandacht binnen de sector. Nederland kent relatief weinig wettelijke eisen voor de beveiliging van energiecentrales.	Naast het primaire belang van levering spelen ook privacybelangen bij het invoeren van slimme meters.
Banken blijven enigszins kwetsbaar voor phishingaanvallen. Bij DDoS zullen pas (zeer) grote en langdurige aanvallen tot schade leiden. Mitigatie wordt dan lastig.	Er wordt veel geïnvesteerd in fraudemanagement (zoals detectie en forensisch onderzoek). De sector heeft effectieve anti-DDoS-maatregelen getroffen die de beschikbaarheid van het betalingsverkeer ten goede komen. Banken onderzoeken additionele maatregelen voor 'als alle andere maatregelen falen', bij heel grote aanvallen. Financiële instellingen delen met regelmaat informatie over voorgekomen DDoS-incidenten. Financiële instellingen toetsen regelmatig hun DDoS-mitigatiemaatregelen.	Het monitoren van potentiële fraudegevallen is een continu proces bij de financiële instellingen. Financiële instellingen blijven gefocust op het verbeteren van het monitoringsproces. Ook het verder uitrollen van "what you see is what you sign"-oplossingen voor ondertekening en authenticatie werkt preventief. De beschikbaarheid van het financiële verkeer is cruciaal. Daarom is er grote aandacht voor afwenden van DDoS-aanvallen.
Privacybescherming en het gebruik van encryptie bemoeilijken het effectief monitoren van netwerkverkeer. Aanvallen zijn dan lastiger te detecteren.	Samenwerking voor cybersecurity gaat goed. Daarin is Nederland uniek in de wereld. Ook worden er meer cybersecurityprofessionals opgeleid. Men ziet blind vertrouwen in de waarde van securitycertificering als een risico.	De sector vormt een belangrijke schakel in veel ketens. Eventuele problemen kunnen zo een risico vormen voor veel maatschappelijke processen in Nederland. Men noemt de zorg en het betalingsverkeer.

Sector	Manifestaties	Dreigingen: actoren	Dreigingen: middelen
Nucleair	De waargenomen manifestaties zijn generiek (phishing, malware) en lijken niet gericht op de sector.	Statelijke actoren en interne actoren (ontstemde medewerkers) zijn de belangrijkste dreigingen voor de sector. Criminelen vormen een dreiging voor de kantoorautomatisering.	De kantoorautomatisering heeft te stellen met cryptoware. Daarnaast ziet men veel (spear)phishing en andere malware. Specifieke ICS-malware is nog niet in de sector waargenomen.
Rijksoverheid	De sector kampt met regelmatige cryptoware-infecties en zwaardere en frequentere DDoS-aanvallen. Cryptoware komt voornamelijk binnen via privémail van medewerkers. Spearphishing richt zich op sleutelposities binnen de overheid, bijvoorbeeld inkopers.	De sector ziet vooral dreiging uitgaan van statelijke actoren en criminelen. Daarnaast vormen interne actoren een belemmering voor cybersecurity. Hun motivatie kan financieel gewin zijn, maar ook ideologische motieven komen voor.	Krachtige aanvalsmiddelen zijn eenvoudiger beschikbaar voor de 'gewone' crimineel. Er vinden regelmatig gerichte aanvallen plaats, waarbij de hele handel en wandel van een medewerker in kaart wordt gebracht. Die informatie wordt gebruikt voor een snelle aanval met niet-digitale gevolgen.
Telecom	Organisaties hebben geregeld te maken met cryptowarebesmettingen, vooral via privémail van medewerkers. Daarnaast vindt er spearphishing plaats gericht op personen in security- en managementfuncties.	Sectorspecifieke dreigingen gaan vooral uit van statelijke actoren. Men ziet daarnaast generieke aanvallen door criminelen (bijvoorbeeld met cryptoware). Als de gebruikers het netwerk overbelasten, zou je ook van een dreiging voor beschikbaarheid kunnen spreken.	Er wordt veel gebruik gemaakt van cryptoware door aanvallers, meer dan er in de media te zien is. DDoS-aanvallen blijven een aandachtspunt. Ook is er nog veel sprake van spam.
Transport (haven, luchthaven, spoor)	Er vinden wel incidenten plaats, maar het koppelen van de gebeurtenis (bijvoorbeeld gestolen containers) aan een digitale aanval blijft lastig. Spearphishingaanvallen zijn soms erg gericht en geavanceerd. Ook zijn er meerdere cryptoware-infecties waargenomen.	Voor de sector vormen criminelen de grootste dreiging. Door het manipuleren van informatie kunnen zij bijvoorbeeld goederen smokkelen of weten waar waardevolle goederen te stelen zijn.	De sector ziet de aandacht van aanvallers voor procescontrolesystemen toenemen. Daarnaast bedienen aanvallers zich van cryptowareaanvallen en (spear)phishing.
Verzekeraars	Er worden gerichte aanvallen waargenomen op verzekeraars. Soms vindt afpersing plaats met dreiging van publicatie van zogenaamd gestolen klantgegevens. Phishing, cryptoware en DDoS-aanvallen blijven plaatsvinden.	De sector heeft voornamelijk te maken met dreiging van criminelen.	Actoren maken gebruik van cryptoware, tooling voor DDoS-aanvallen, malware en phishing.
Zorg	Men ziet een duidelijke stijging van het aantal cryptoware-incidenten. Soms worden zelfs niet aan internet gekoppelde systemen geïnfecteerd met besmette USB-sticks. Ook ziet men soms 'interne' hackpogingen van patiënten.	De grootste dreiging gaat voor de sector uit van statelijke actoren (spionage van onderzoeksgegevens) en interne medewerkers die ongeautoriseerd toegang krijgen tot gegevens. Criminelen lijken nog maar beperkt interesse te hebben in medische gegevens.	Cryptoware-aanvallen zijn populair maar lijken niet echt sectorspecifiek. Phishing vindt veel plaats. Regelmatig gaat het hier om erg specifieke aanvallen, bijvoorbeeld op een persoon of afdeling gericht.

Weerbaarheid: kwetsbaarheden	Weerbaarheid: maatregelen	Belangen
Er zijn geen relevante ontwikkelingen.	De maatregelen van de sector worden door de overheid getoetst tegen het DBT Cybersecurity. Er zijn internationale initiatieven van IAEA om cybersecurity in de sector verder te verbeteren. De sector werkt intensiever samen met het NCSC. Daarnaast is de cybercomponent van het Alerteringssysteem Terrorismebestrijding ten uitvoer gebracht.	De rol van ICT binnen de sector is vooral ondersteunend, bijvoorbeeld bij het regelen van toegangsbeveiliging. Het belang van nucleaire veiligheid geldt als bekend.
De sector geeft aan dat de brede verspreiding van (persoons)gegevens binnen de overheid niet altijd gepaard gaat met bijbehorende overdracht van verantwoordelijkheden voor de beveiliging ervan.	Er is een afname van het gebruik van BYOD ten faveure van door de organisatie beheerde ICT.	De overheid dient een breed scala aan belangen die afhankelijk zijn van ICT. Te denken valt aan burgers voor wie het primaire inkomen ervan afhangt (UWV, SVB), het effectief optreden van politie en justitie of het keren en beheren van oppervlaktewater.
Er is soms sprake van een monocultuur omdat sommige ICT-leveranciers aan (bijna) alle telecombedrijven leveren. Ook valt het organisaties zwaar steeds 'bij' te blijven met het beveiligen van nieuwe technologieën (zoals 4G, 5G en IPv6).	Men ziet dataminimalisatie als een manier om een minder aantrekkelijk doelwit voor aanvallen te vormen. Daarnaast zijn initiatieven als AbuseHUB (uitwisseling informatie over infecties) en MANRS (afspraken over internet-routering) van grote waarde voor de stabiliteit van het netwerk.	De betrouwbaarheid van het telefonienetwerk is van direct belang voor de maatschappij. Daarnaast zijn er andere systemen die sterk steunen op het netwerk, zoals bij de aansturing van procescontrolesystemen (ICS).
Transportsector wordt gekarakteriseerd door afhankelijkheid van een paar coördinatiepunten. Wet- en regelgeving in de sector maakt daarnaast processen vaak afhankelijker van ICT. Wordt er vervolgens inbreuk gemaakt op systemen, dan zijn de gevolgen groter.	Men ziet awareness groeien, ook op bestuurlijk niveau. Ook vanuit de overheid is er meer interesse voor het voldoende beveiligen van infrastructuren.	Korte verstoringen kunnen economische gevolgen hebben omdat transporten uitwijken naar andere landen. Langdurige verstoringen kunnen leiden tot problemen bij de voedsel-voorziening.
Actoren richten zich specifiek op fraude langs digitale weg. Door de ingezette verschuiving naar online dienstverlening, vormen internet-kwetsbaarheden en misbruik daarvan een steeds groter risico bij verzekeraars, gevolmachtigden en tussenpersonen.	De sector werkt structureel aan verhoging en instandhouding van het volwassenheidsniveau van securitymaatregelen. Hierbij wordt rekening gehouden met een continu evoluerend risicolandschap. Hierop vindt toezicht plaats vanuit DNB.	De sector is langs digitale weg verantwoordelijk voor omvangrijke geldstromen en financiële transacties en verwerkt veel gevoelige gegevens van burgers. Financiële schade van een verzekeraar heeft indirecte gevolgen voor de premie van verzekerden. Individuele incidenten kunnen een weerslag hebben op de reputatie van de gehele sector.
Het 'eigen initiatief' van medisch specialisten (die eigen databases opzetten) of medicijnfabrikanten (die eigen apps leveren) maakt beveiligen lastig. Men vindt dat er onvoldoende (zorgvuldig) dataclassificatie wordt toegepast.	De oprichting van de Zorg-ISAC leidt tot belangrijke samenwerking voor beveiliging van gegevens. De meldplicht datalekken en aandacht van raden van bestuur en toezicht zorgen ervoor dat het onderwerp op de bestuursagenda komt.	De sector is verantwoordelijk voor de kwaliteit van patiëntenzorg. De kwaliteit en vertrouwelijkheid van patiëntgegevens is daarbij een belangrijke randvoorwaarde.

Bijlage 3 Afkortingen- en begrippenlijst

0-day	Zie Zero-daykwetsbaarheid.
2G/3G/4G	Verschillende generaties van mobiele communicatie. In Nederland staan deze generaties synoniem voor gsm (2G), UMTS (3G) en lte (4G).
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
APT	Een Advanced Persistent Threat (APT) is een gemotiveerde (soms geavanceerde) doelgerichte aanval op een natie, organisatie, persoon of groep van personen.
Authenticatie	Authenticatie is het nagaan of een bewijs van identiteit van een gebruiker, computer of applicatie overeenkomt met vooraf vastgelegde echtheidskenmerken.
Bitcoin	Munteenheid, zie cryptocurrency.
Booterservice	Online dienst die tegen betaling DDoS-aanvallen uitvoert voor actoren zonder technische kennis.
Bot/Botnet	Een bot is een geïnfecteerde computer die op afstand, met kwade bedoelingen, bestuurd kan worden. Een botnet is een verzameling van dergelijke geïnfecteerde computers die centraal bestuurd kan worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.
BSI	Het Bundesamt für Sicherheit in der Informationstechnik (BSI) is de Duitse overheidsdienst voor verbindings- en informatiebeveiliging.
BYOD	Bring Your Own Device (BYOD) is een regeling in organisaties waarbij personeel eigen consumentenapparatuur kan gebruiken voor het uitvoeren van de taken voor de organisatie.
Certificaat	Een certificaat is een bestand dat fungeert als digitale identificatie van een persoon of systeem. Het bevat ook PKI-sleutels om gegevens tijdens transport te versleutelen. Een bekende toepassing van certificaten zijn de met https beveiligde websites.
Certificaatautoriteit	Een certificaatautoriteit (CA) in een PKI-stelsel is een organisatorisch verband dat wordt vertrouwd om certificaten te maken (genereren), toe te wijzen en in te trekken.
C&C	Een Command & Control (C&C)-server is een centraal systeem in een botnet van waaruit het botnet wordt aangestuurd.
Cloud/Clouddiensten	Een op internet (de 'wolk') gebaseerd model voor systeemarchitectuur, waarbij vooral gebruikgemaakt wordt van Software as a Service (SaaS).
CMS (Content Management System)	Een contentmanagementsysteem is een softwaretoepassing waarmee gebruikers zonder veel technische kennis documenten en gegevens kunnen plaatsen op een website.
Cryptocurrency	Verzamelnaam voor digitale munteenheden waarbij cryptografische berekeningen als echtheidskenmerk en voor transacties worden gebruikt. De bitcoin is daarbij de meest-voorkomende.
Cryptoware	Type ransomware dat bestanden op een computer of in een netwerk versleutelt. De sleutel wordt alleen tegen betaling vrijgegeven.

Cybercrime	Vorm van criminaliteit gericht op een ICT-systeem of de informatie die daardoor wordt verwerkt.
Cybercrimineel	Actoren die beroepsmatig cybercrime plegen met hoofdzakelijk geldelijk gewin als doel. Het CSBN onderscheidt de volgende groepen cybercriminelen: • in enge zin, zij die zelf aanvallen plegen (of daarmee dreigen) om geld te verdienen; • criminele digitale dienstverleners, zij die diensten en tools aanbieden waardoor of waarmee anderen digitale aanvallen kunnen uitvoeren; • handelaren in of dienstverleners voor gestolen informatie; • criminelen die digitale aanvallen gebruiken voor traditionele criminaliteit.
Cyberonderzoeker	Actor die op zoek gaat naar kwetsbaarheden en/of inbreekt in ICT-omgevingen om de (te) zwakke beveiliging ervan aan de kaak te stellen.
Cybersecurity	Het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.
Datalek	Het opzettelijk of onopzettelijk naar buiten komen van vertrouwelijke gegevens.
(D)DoS	(Distributed) Denial of Service is de benaming voor een type aanval die een bepaalde dienst (bijvoorbeeld een website) onbereikbaar maakt voor de gebruikelijke afnemers. Een DoS op een website wordt vaak uitgevoerd door de website te bestoken met veel netwerkverkeer, waardoor deze onbereikbaar wordt.
DigiD	De digitale identiteit van burgers, waarmee ze zich identificeren en authenticeren op websites van de overheid. Zo weten overheidsinstellingen dat ze echt met een bepaalde burger te maken hebben.
DKIM	DomainKeys Identified Mail is een protocol om legitieme e-mail door de verzendende mailserver digitaal te laten ondertekenen. De eigenaar van het verzendende domein publiceert legitieme sleutels in een DNS-record.
DMARC	Domain-based Message Authentication, Reporting, and Conformance is een protocol waarmee de eigenaar van een domein aangeeft wat er met niet-authentieke e-mail vanaf zijn domein moet gebeuren. De authenticiteit van de e-mail wordt eerst vastgesteld aan de hand van SPF en DKIM. De domeineigenaar publiceert het gewenste beleid in een DNS-record.
DNS	Het Domain Name System (DNS) is het systeem dat internetdomeinnamen koppelt aan IP-adressen en omgekeerd. Zo staat het adres 'www.ncsc.nl' bijvoorbeeld voor IP-adres '62.100.52.106'.
DNSSEC	DNS Security Extensions (DNSSEC) is een uitbreiding op DNS waarbij een authenticiteits- en integriteitscontrole wordt toegevoegd aan het bestaande systeem.
Dreiging	Het Cybersecuritybeeld Nederland definieert doel en dreiging als volgt: Het hogere doel (intentie) kan zijn het verstevigen van de concurrentiepositie; politiek/landelijk gewin, maatschappelijke ontwrichtingof levensbedreiging. Dreigingen in het beeld zijn onder andere ingedeeld als: digitale spionage, digitale sabotage, publicatie van vertrouwelijke gegevens, digitale verstoring, cybercrime en indirecte verstoringen.
Encryptie	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden.
End-of-life	In de softwarewereld betekent de end-of-life van een product de datum waarop een product niet langer door de leverancier als gangbare software wordt beschouwd. Als software end-of-life is, maakt de leverancier over het algemeen geen updates meer en levert hij ook geen ondersteuning.
ENISA	Europees Agentschap voor netwerk- en informatiebeveiliging

EMV	Europay Mastercard Visa (EMV) is een standaard voor betaalkaartsystemen op basis van chipkaarten en chipkaartbetaalterminals. De chipkaart vervangt kaarten met een magneetstrip, die makkelijk te kopiëren zijn.
Exploit	Software, gegevens of opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software of hardware om ongewenste functies en/of gedrag te veroorzaken.
Exploitkit	Hulpmiddel van een actor om een aanval op te zetten door te kiezen uit kant-en-klare exploits, in combinatie met gewenste gevolgen en besmettingsmethode.
GCHQ	Government Communications Headquarters (Britse inlichtingendienst)
Gevoelige informatie	Gegevens over kritieke (vitale) infrastructuur die, wanneer zij openbaar worden gemaakt, gebruikt kunnen worden om plannen te maken en feiten te plegen om kritieke infrastructuurinstallaties te verstoren of te vernietigen.
Hacker/Hacken	De meest gangbare en de in dit document gehanteerde betekenis van hacker is iemand die met kwaadaardige bedoelingen probeert in te breken in computersystemen. Oorspronkelijk werd de term hacker gebruikt voor iemand die op onconventionele wijze gebruikmaakt van techniek (waaronder software), veelal om beperkingen te omzeilen of onverwachte effecten te bereiken.
Hacktivist	Samentrekking van hacker en activist: personen of groepen die uit ideologische motieven digitale aanvallen van activistische aard plegen.
Hashing	Hashing is een cryptografische bewerking om gegevens onomkeerbaar te verhaspelen. Hashing wordt gebruikt om wachtwoorden zo op te slaan dat ze na een datalek moeilijker te misbruiken zijn.
Hulpmiddel	Een techniek of computerprogramma waarmee een aanvaller misbruik kan maken van bestaande kwetsbaarheden of deze kan vergroten.
ICS	Industriële controlesystemen (ICS) (ook Supervisory Control And Data Acqusition (SCADA) genoemd) zijn meet- en regelsystemen, bijvoorbeeld voor de aansturing van industriële processen of gebouwbeheersystemen. ICS'en verzamelen en verwerken meet- en regelsignalen van sensoren in fysieke systemen en regelen de aansturing van de bijbehorende machines of apparaten.
Identiteitsfraude	Het opzettelijk misbruik maken van de identiteitsgegevens van iemand anders om daarmee fraude te plegen.
Incident	Een incident is een ICT-verstoring in de dienstverlening waardoor de te verwachten beschikbaarheid van de dienstverlening geheel of gedeeltelijk is verdwenen en/of het ongeoorloofd openbaren, verkrijgen en/of wijzigen van informatie.
Informatiebeveiliging	Het proces van vaststellen van de vereiste kwaliteit van informatie(systemen) in termen van vertrouwelijkheid, beschikbaarheid, integriteit, onweerlegbaarheid en controleerbaarheid alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende (fysieke, organisatorische en logische) beveiligingsmaatregelen.
Integriteit	Een kwaliteitskenmerk voor gegevens, een object of dienst in het kader van de (informatie)beveiliging. Het is een synoniem voor betrouwbaarheid. Een betrouwbaar gegeven is juist (rechtmatigheid), volledig (niet te veel en niet te weinig), tijdig (op tijd) en geautoriseerd (gemuteerd door een persoon die gerechtigd is de mutatie aan te brengen).
Interne actor	Individueel persoon of groep in een organisatie die daar van binnenuit cybersecurityincidenten veroorzaakt.
Internet der Dingen	Fenomeen waarbij het internet niet alleen wordt gebruikt om gebruikers toegang te bieden tot websites, e-mail en dergelijke, maar om apparaten aan te sluiten die het gebruiken voor functionele communicatie.

IP	Het Internet Protocol (IP) zorgt voor adressering van datapakketten, zodat ze bij het beoogde doel aankomen.
IPv4/IPv6	IPv4 is een versie van IP met een adresruimte van ruim vier miljard adressen. IPv6 is de opvolger daarvan, met 3,4 keer 10^{38} mogelijke adressen. Dat zijn vijftig miljard keer miljard keer miljard adressen per persoon op aarde.
ISAC	Een Information Sharing and Analysis Centre (ISAC) is een samenwerkingsverband tussen organisaties voor het uitwisselen van (dreigings)informatie en gezamenlijke weerbaarheidsverhoging. Het NCSC faciliteert meerdere ISAC's voor vitale sectoren in Nederland.
Kwetsbaarheid	Eigenschap van een samenleving, organisatie of informatiesysteem (of een onderdeel daarvan) die een kwaadwillende partij de kans geeft om de legitieme toegang tot informatie of functionaliteit te verhinderen en te beïnvloeden, of om die ongeautoriseerd te benaderen.
Malvertising	Het verspreiden van malware door die aan een advertentiebemiddelaar aan te bieden, zodat grote groepen gebruikers worden besmet via legitieme websites.
Malware	Samentrekking van 'malicious' en 'software', kwaadaardige software. Malware is de term die tegenwoordig als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en Trojaanse paarden.
MitM	Man-in-the-middle (MitM) is een aanvalstechniek waarbij de aanvaller zich tussen twee partijen bevindt, bijvoorbeeld een internetwinkel en een klant. De aanvaller doet zich richting de klant voor als de winkel en andersom. Als tussenpersoon kan de aanvaller uitgewisselde gegevens afluisteren en/of manipuleren.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid, onderdeel van het Ministerie van Veiligheid en Justitie
NTP	Het Network Time Protocol (NTP) is een populair protocol voor het automatisch instellen van de tijd op een systeem.
Patch	Een patch (letterlijk: pleister) kan bestaan uit reparatiesoftware of kan wijzigingen bevatten die direct in een programma worden doorgevoerd om dat programma te repareren of te verbeteren.
Phishing	Verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan worden misbruikt voor bijvoorbeeld identiteitsdiefstal of creditcardfraude. Spearphishing is een variant die zich richt op één persoon, of een zeer beperkte groep personen, die specifiek worden uitgekozen op basis van hun toegangspositie om een zo groot mogelijk effect te sorteren zonder al te veel op te vallen.
PKI	Een Public Key Infrastructure (PKI) is een verzameling organisatorische en technische middelen waarmee iemand op een betrouwbare manier een aantal zaken kan regelen, zoals het versleutelen en ondertekenen van informatie en het vaststellen van de identiteit van een andere partij.
PoS	Een Point-of-Sale (PoS) of kassasysteem is een computer waarop verkooptransacties worden geregistreerd.
Ransomware	Type malware dat systemen en informatie daarop blokkeert en alleen tegen betaling van losgeld toegankelijk maakt.
RAT	Een Remote Access Tool (soms Remote Access Trojan, RAT) wordt gebruikt voor het verkrijgen van toegang tot de computer van een doelwit om die op afstand te kunnen bedienen.

Responsible disclosure	Praktijk van het verantwoord melden van aangetroffen beveiligingslekken. Hierbij worden afspraken gehanteerd die doorgaans neerkomen op dat de melder de ontdekking niet deelt met derden totdat het lek verholpen is, en de getroffen partij geen juridische stappen tegen de melder zal ondernemen.
SCADA	Zie ICS.
Scriptkiddie	Actor met beperkte kennis die hulpmiddelen gebruikt die door anderen zijn bedacht en ontwikkeld, voor digitale aanvallen van baldadige aard.
SIDN	Stichting Internet Domeinregistratie Nederland
Skimmen	Het onrechtmatig kopiëren van de gegevens van een elektronische betaalkaart, bijvoorbeeld een pinpas of creditcard. Skimmen gaat vaak gepaard met het bemachtigen van pincodes, met als uiteindelijk doel betalingen te verrichten of geld op te nemen van de rekening van het slachtoffer.
Social engineering	Een aanvalstechniek waarbij misbruik wordt gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht om vertrouwelijke informatie te verkrijgen of het slachtoffer een bepaalde handeling te laten verrichten.
Spearphishing	Zie phishing.
SPF	Sender Policy Framework is een protocol waarmee de eigenaar van een domeinnaam aangeeft welke servers er legitiem e-mail namens zijn domein mogen versturen. De domeinnaameigenaar publiceert de lijst met geautoriseerde servers in een DNS-record.
SQL-injectie	Aanvalstechniek waarmee de aanvaller de communicatie tussen een applicatie en de achterliggende database kan beïnvloeden. Het doel is om gegevens in de database te manipuleren of te stelen.
Statelijke actor	Er is sprake van een statelijke actor als de actor handelt uit naam van een nationale overheid.
Steganografie	Techniek om gegevens te verbergen door ze te verwerken in een andere gegevensstroom, zoals in afbeeldingen of geluidsbestanden.
TCP	Transmission Control Protocol
Terrorist	Actor met ideologische motieven die maatschappelijke veranderingen probeert te bewerkstelligen, bevolking(sgroepen) angst wil aanjagen of politieke besluitvorming probeert te beïnvloeden, door geweld tegen mensen te gebruiken of ontwrichtende schade aan te richten.
THTC	Team High Tech Crime (politie)
TLS	Transport Layer Security is een protocol voor het opzetten van een beveiligde verbinding tussen twee computersystemen. TLS vormt de basis van het https-protocol. TLS is de opvolger van Secure Sockets Layer (SSL).
Tweefactorauthenticatie	Een manier van authenticeren waarvoor twee onafhankelijke bewijzen van identiteit zijn vereist.
UDP	User Datagram Protocol
USB	Universal Serial Bus (USB) is een specificatie van een standaard van de communicatie tussen een apparaat, in veel gevallen een computer, en randapparatuur.
USB-stick	Draagbaar opslagmedium dat via een USB-aansluiting aan computers kan worden gekoppeld.
Vertrouwelijkheid	Een kwaliteitskenmerk van gegevens in het kader van de informatiebeveiliging. Met vertrouwelijkheid wordt bedoeld dat een gegeven alleen te benaderen is door iemand die ertoe gerechtigd is. Dit wordt vastgesteld door de eigenaar van de gegevens.

VPN	Een Virtual Private Network (VPN) is een geïsoleerde, versleutelde verbinding tussen een apparaat en een bepaalde server op het internet. Dit kan worden toegepast om veilig bedrijfs- of internettoegang te verkrijgen vanaf niet-vertrouwde netwerken.
Wateringhole	Een wateringhole-aanval is gericht op een plek waar veel beoogde slachtoffers samenkomen. De aanvaller verspreidt zijn exploit of malware via een website die zij regelmatig bezoeken door misbruik te maken van een kwetsbaarheid in deze website of een CMS waarop de website gebaseerd is.
Webapplicatie	Het geheel van software, databases en systemen dat betrokken is bij het correct functioneren van een website. De website is het zichtbare gedeelte.
Weerbaarheid	Het vermogen van personen, organisaties of samenlevingen om weerstand te bieden aan negatieve invloeden op de beschikbaarheid, vertrouwelijkheid en/of integriteit van (informatie)systemen en digitale informatie.
Zero-daykwetsbaarheid	Een zero-daykwetsbaarheid is een kwetsbaarheid waarvoor nog geen patch beschikbaar is omdat de maker van de kwetsbare software nog geen tijd heeft gehad om een patch te maken.

Uitgave
Nationaal Cyber Security Centrum
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 55 55

Meer informatie
www.ncsc.nl
csbn@ncsc.nl

September 2015